Mérési jegyzőkönyv

Ethernet és TCP/IP protokollok vizsgálata

V03b (2014.01.28.)

A feladatokat összeállította: Kovácsházy Tamás, BME MIT, 2008-2010.
A jegyzőkönyvsablont módosította: Tóth Csaba, BME MIT, 2011.
A feladatokat és a sablont módosította: Huszerl Gábor, BME MIT, 2012-2013.
A jegyzőkönyvsablont módosította: Tóth Csaba, BME MIT, 2014.

A mérés helyszíne:	**I.B141/IB142, ... mérőhely**
A mérés időpontja:	**2014. február 4.**
A mérést végezték:	**Varga Domonkos**
Ennek a fájlnak a neve:	**fájlnév** **ml4_vargad_1.doc**
A mérésvezető neve:	**Naszály Gábor**

Tudnivalók:

- Csak a világossárga színnel jelölt részekre írjon! A fejlécet értelemszerűen töltse ki.
- A <<... képernyőkép>> emlékeztető szöveg helyére vagy alá illessze be a feladat megoldását igazoló képernyőképet!
- A feladatok egy részét az ellenőrzőmérésen csak az ötös osztályzathoz kell megoldani, ezeket *-gal jelöltük.
- A feladatok egy része fakultatív, ezek nem számítanak bele az értékelésbe, csak ha marad idő, akkor fogjanak hozzá! (Cserébe viszont szakmailag érdekesek.)
- A méréssekkel kapcsolatos észrevételeit jelezze a mérésvezetőnek vagy a tárgyfelelősnek (toth AT mit.bme.hu)!

1. feladat: Ethernet és TCP/IP beállítások megismerése

A feladat célja: Ethernet hálózati interfészek alapvető TCP/IP beállításainak megismerése az **`ipconfig`** és a **`route print`** program segítségével.

1.1. A számítógép (PC) hálózati interfészei és beállításai

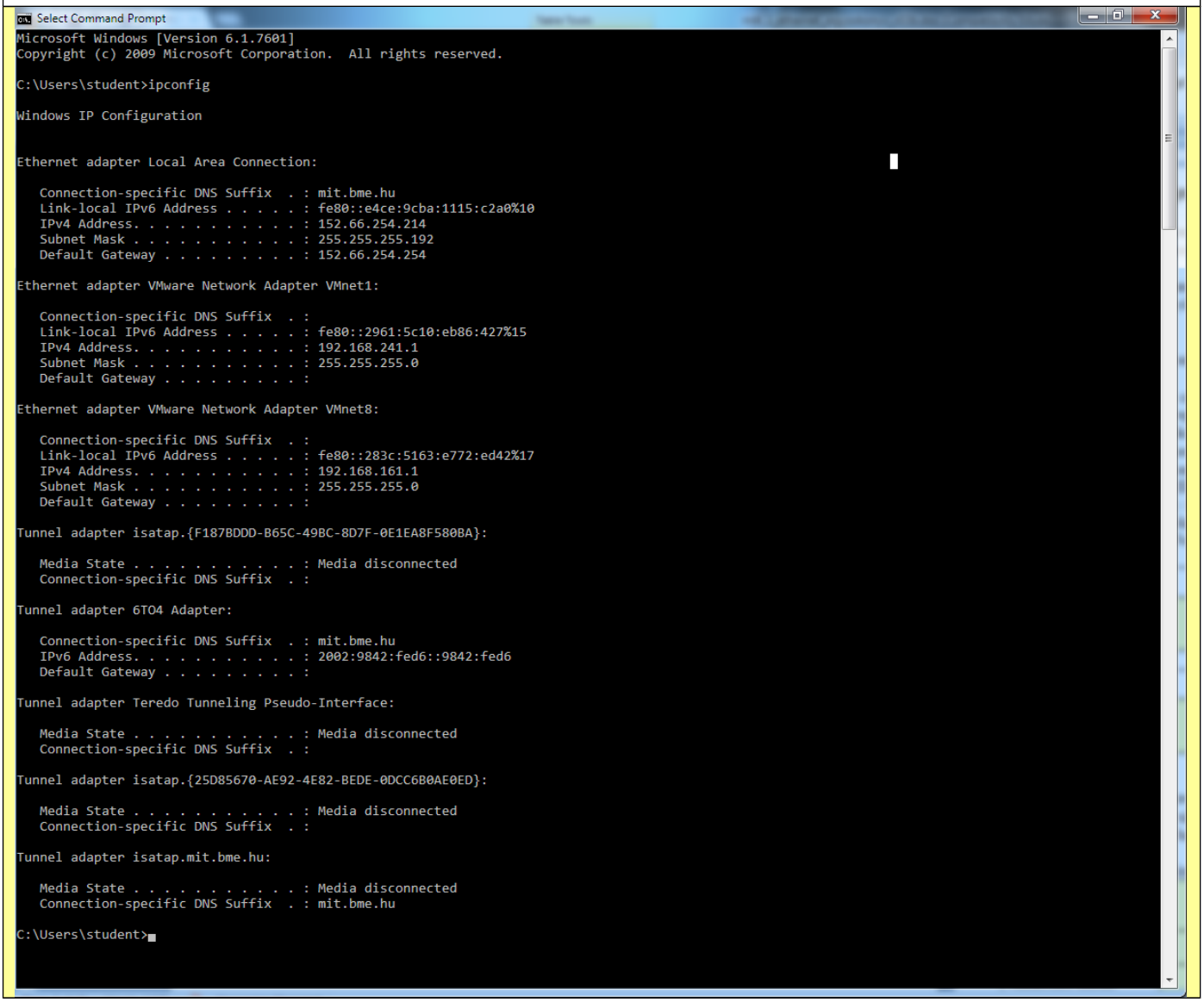
Állapítsa meg, hogy milyen hálózati interfészei vannak a mérés során használt számítógépnek, majd határozza meg az egyes interfészek hálózati beállításait!

Adja ki a Windows Command Prompt ablakban az **`ipconfig`** majd az **`ipconfig /all`** parancsot, és másolja be a kapott képernyőábrát a jegyzőkönyvbe!

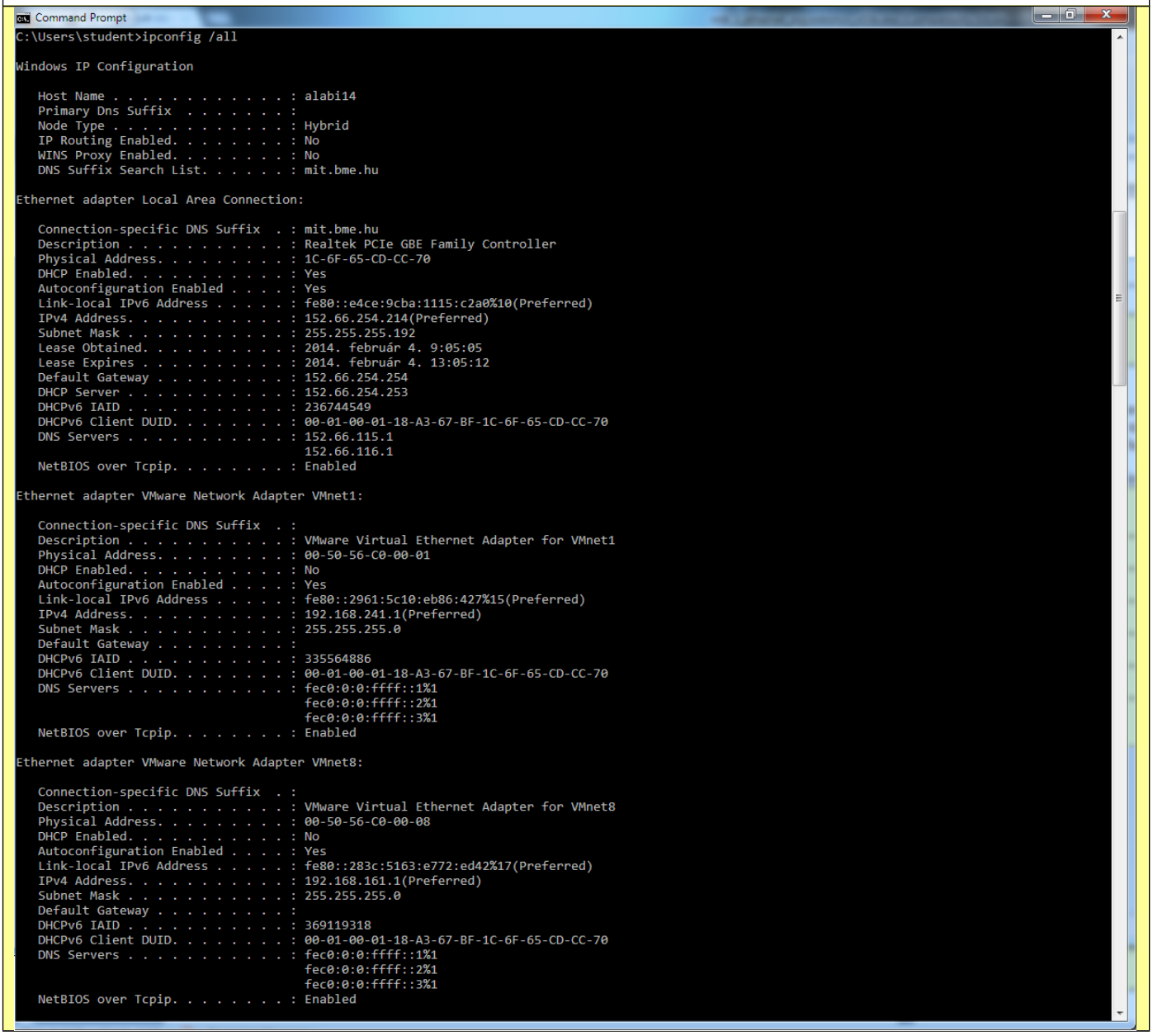
Tanácsok:

- A **`cd \`** paranccsal váltson át a gyökérkönyvtárba, hogy a fölösleges könyvtári útvonal ne zavarjon!
- A command ablak csúszkájával és a command ablak magasságával állítsa be úgy az ablakot, hogy csak a kívánt szövegrész látszódjék, és ALT+Pint Screen-nel másolja ki az ablak tartalmát, majd illessze be a jegyzőkönyv megfelelő helyére CTRL+V-vel!
- Egy másik, nehézkesebb és kevésbé látványos megoldás, de hosszú szövegeknél szükség lehet rá: másolja ki a command ablakból a vonatkozó szöveget, és formázza olvashatóra a jegyzőkönyvben! (Ehhez a command ablak jobb egérgombos felugró menüjében válassza ki a Megjelölés (Mark) funkciót, jelölje ki az ablak tartalmának átmásolandó részét, és Enterrel másolja be a vágólapra a kijelölt részt, majd a CTRL+V-vel másolja be a jegyzőkönyvbe a megfelelő helyre! Ne feledkezzen meg a formázásról!)

ipconfig


Select Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\student>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : mit.bme.hu
Link-local IPv6 Address . . . . . : fe80::e4ce:9cba:1115:c2a0%10
IPv4 Address. . . . . : 152.66.254.214
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 152.66.254.254
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2961:5c10:eb86:427%15
IPv4 Address. . . . . : 192.168.241.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::283c:5163:e772:ed42%17
IPv4 Address. . . . . : 192.168.161.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Tunnel adapter isatap.{F187BDDD-B65C-49BC-8D7F-0E1EA8F580BA}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter 6TO4 Adapter:
Connection-specific DNS Suffix . : mit.bme.hu
IPv6 Address. . . . . : 2002:9842:fed6::9842:fed6
Default Gateway . . . . . :
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter isatap.{25D85670-AE92-4E82-BEDE-0DCC6B0AE0ED}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter isatap.mit.bme.hu:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : mit.bme.hu
C:\Users\student>

ipconfig /all



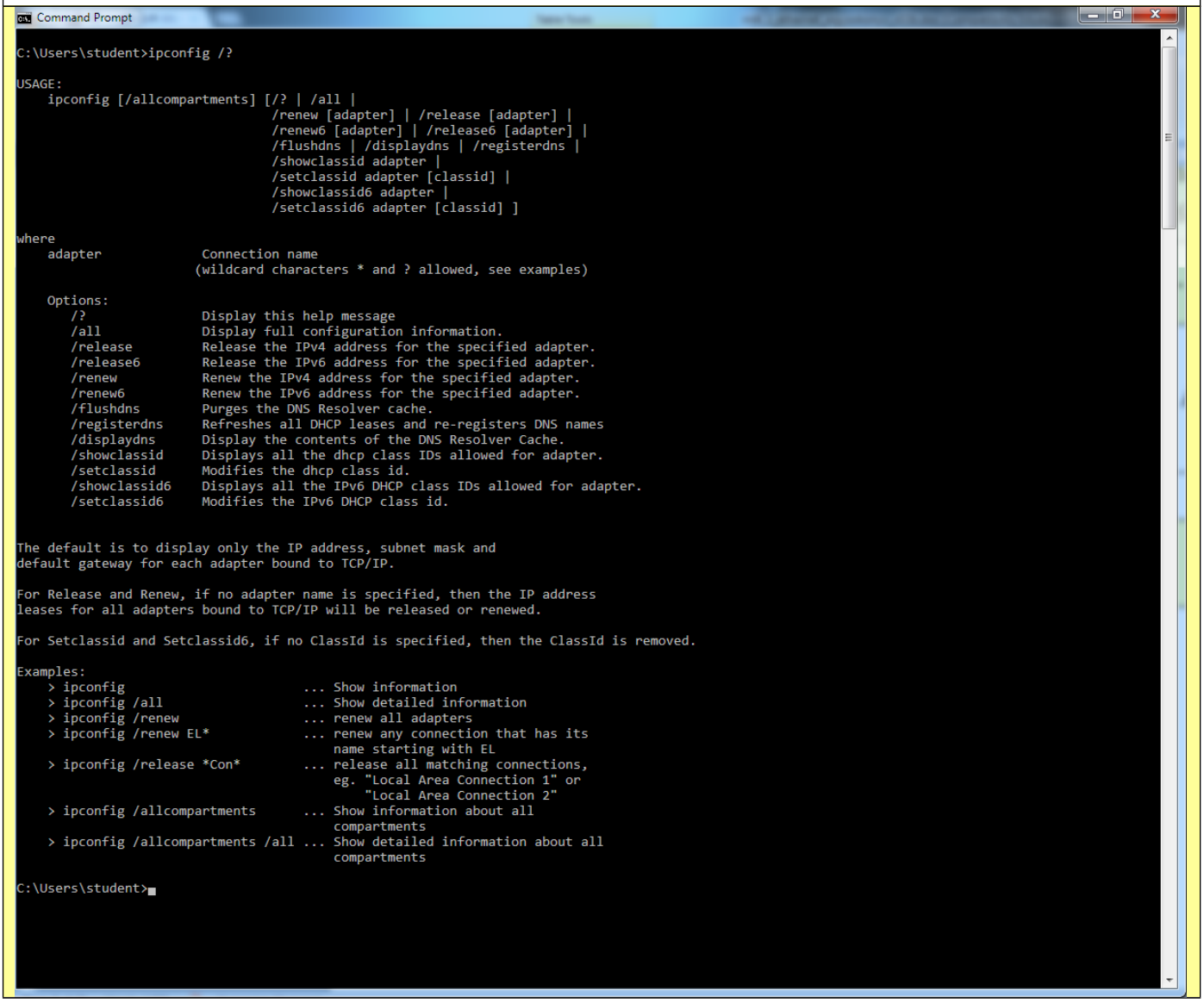
Elemezze és hasonlítsa össze az **`ipconfig`** és az **`ipconfig/all`** parancsra kapott válaszokat, és ezek alapján töltse ki az alábbi táblázatot! (A tunnel adapterekkel ne foglalkozzon, azok az IPv6-os funkciók IPv4-es környezetben való használatát támogatják. A mérésen nem használjuk őket.)

Hálózati interfészek beállításai:

Név	***Ethernet adapter Local Area Connection***	***Ethernet adapter VMware Network Adapter VMnet1***	***Ethernet adapter VMware Network Adapter VMnet8***
IP cím	152.66.254.214	192.168.241.1	192.168.161.1
Alhálózati maszk	255.255.255.192	255.255.255.0	255.255.255.0
Alapértelmezett átjáró	152.66.254.254	----------	----------
DHCP engedélyezve	Igen	Nem	Nem
DNS szerverek	152.66.115.1 152.66.116.1	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1
Kapcsolatspecifikus DNS utótag	mit.bme.hu	----------	----------

Nézze meg az **`ipconfig`** parancs egyéb paramétereit is az **`ipconfig /?`** segítségével!
(Pl. a **`/flushdns`**-re szükség lesz a további mérésekben.)

`ipconfig /?`



1.2. IP címtartományok

Mi a laborban használható IP címek tartománya?

IP címtartomány:	152.66.254.193 - 152.66.254.254

1.3. Default gateway, subnet broadcast IP cím és a DHCP szerver címe

Mi az alapértelmezett átjáró (default gateway), a subnet broadcast IP cím és a DHCP szerver címe?

	IP-cím
Alapértelmezett átjáró:	152.66.254.254
Subnet broadcast:	152.66.254.255
DHCP szerver:	152.66.254.253

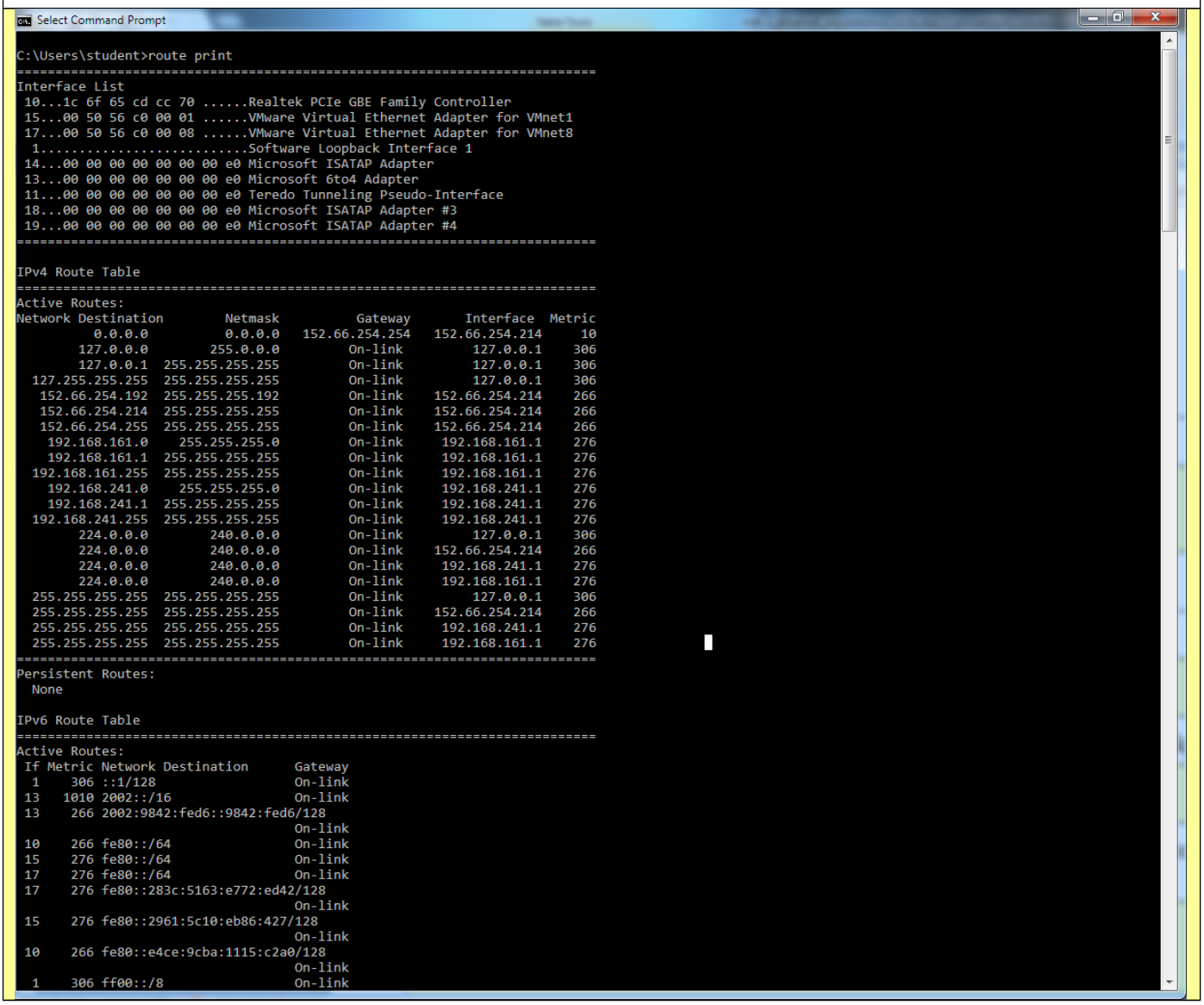
1.4. DNS szerver

Mely DNS szervereket használja a gép? Mire kellenek ezek? (IP-cím, definíció)
152.66.115.1 152.66.116.1 A domain névhez társítják a megfelelő IP címet.
Miért szükséges több DNS szervert megadni?
A redundancia miatt.
Miért nem domain nevükkel adtuk meg a DNS szervereket?
A domain – IP cím fordítás miatt nem.

1.5. Internet útvonalak

Futtassa le a **`route print`** parancsot!
(A válasznak csak az „IPv4 Route Table” részével foglakozzanak.)

`route print`



Magyarázza meg a program kimenetét![1]
A route print kimenete azt adja meg, hogy az IP cím alapján melyik interfészen lesz kiküldve a célállomáshoz.
Hogyan használja fel ezt az információt a számítógép TCP/IP protokoll-stackje?
A csomagokat ez alapján továbbítják.

[1] A Windowsban használt útvonalválasztásról itt találhat leírást: TCP/IP Fundamentals for Microsoft Windows, Chapter 5 IP Routing, **http://technet.microsoft.com/en-us/library/bb727001.aspx#EEAA**

Mik a kimenetben megjelenő **0.0.0.0** és **127.0.0.0** IP címekhez tartozó bejegyzések, és mikor/mire használják azokat?

0.0.0.0:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	152.66.254.254	152.66.254.214	10

127.0.0.0:

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306

Mik a **224.0.0.0** IP címekhez tartozó bejegyzések?

224.0.0.0:

224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	152.66.254.214	266
224.0.0.0	240.0.0.0	On-link	192.168.241.1	276
224.0.0.0	240.0.0.0	On-link	192.168.161.1	276

2. feladat: Ethernet címek és összerendelésük IP címekkel

A feladat célja: Ethernet címek és IP címek összerendelésének megértése a **`ping`** program segítségével.

A **`ping`** egy olyan hálózati tesztprogram, amely a paramétereként megadott IP című vagy domain nevű gépnek egy *ICMP Echo Request* üzenetet küld (alapbeállításban négyszer), amelyre a célállomás egy *ICMP Echo Reply* üzenettel válaszol (ha a telepített tűzfal nem tiltja).

A mérés során felhasználjuk az ARP-t (*Address Resolution Protocol*), amely az IP címekhez Ethernet címet rendel. Az ARP implementációk a kérések számának minimalizálására cache-ben tárolják az adatokat (pl. a Windows XP 10 percig tartja meg a bejegyzéseket). Az ARP cache tartalmát az **`arp -a`** paranccsal lehet megnézni, az **`arp -d *`** paranccsal pedig törölni. (Nézze meg az **`arp`** parancs egyéb paraméterezését is (**`arp /?`** segítségével)! A törléshez rendszergazdai jogosultságra van szükség. Ilyet emelt jogosultságú (elevated) command ablak használatával tud szerezni. Ehhez linket az asztalon talál.

Szintén használni fogjuk a DNS-t (Domain Name System), amely a domain nevekhez IP címeket rendel (erről a protokollról később még szó lesz). A Windows a DNS kérések számának minimalizálására fenntart egy DNS cache-t, alapértelmezésben 24 órás tárolási idővel. Az **`ipconfig /displaydns`** kiírja a DNS cache tartalmát, az **`ipconfig /flushdns`** pedig törli.

A mérés könnyítése érdekében a következő feladatokat egy virtuális gépből végezzék. Ezzel a többi mérőpár zavaró mellékhatásaitól tudnak megszabadulni. Indítsák el a VMware Player alkalmazást (taskbar), majd nyissa meg a `2meres_Win2013` nevű virtuális gépet. Ellenőrizze (Edit VM settings), hogy a hálózati adaptere NAT módban legyen, állítsa át erre, ha kell. Indítsa el a virtuális gépet. A `meres` felhasználó jelszava `MeresLabor4`.

A feladat során öt célállomást kell a **`ping`** parancs segítségével megszólítania, rögzíteni mind az öt alkalommal a teljes forgalmat Wireshark programmal, majd a hálózati forgalom elemzésével válaszolni a feltett kérdésekre.

A vizsgálandó gépek, domain nevek:

1. alapértelmezett átjáró (default gateway),
2. a labor DHCP szervere,
3. az alaplabor szervere (alaplab.mit.bme.hu),
4. egy nem létező, fantom.mit.bme.hu domain nevű gép,
5. a subnet broadcast cím.

A mérések előtt minden esetben törölje ki az ARP és DNS cache-t, hogy a protokoll teljes működését meg tudja figyelni! A feladathoz készítsen egy batch file-t! A batch fájl egy egyszerű, **`bat`** vagy **`cmd`** kiterjesztésű szöveges fájl, amelyben minden sorban egy-egy végrehajtandó parancs van. A batch fájlnak átadott paraméterekre a **`%1`**, **`%2`** stb. változókkal lehet hivatkozni.

A mérés menete:

- Készítsen egy batch fájlt, amely törli az ARP és DNS cache-t, és egyúttal kiadja a **`ping`** parancsot! A batch fájlt NE ping-nek nevezze el. Gondolja végig, hogy ez miért lenne rossz ötlet.
- Indítsa el a fizikai gépen Wiresharkban a forgalomrögzítést! Azt a hálózati interface-t figyelje, amelynek IP-címe a virtuális gép alhálózatának címtartományába esik. (A virtuális gép IP beállításai látszanak az asztala háttérképén, a Wiresharkban a hálózati interfészek címe olvasható az interface kiválasztásakor. Az interface címére kattintva válthat az IPv6-os és IPv4-es címek között.)

- A batch fájl segítségével **`ping`**-elje meg a megfelelő gépet/nevet!
- Állítsa le a forgalomrögzítést!
- Másolja be a jegyzőkönyvbe a cmd ablakot!
- Készítsen/alkalmazzon display filtert a Wiresharkhoz a zavaró forgalom kiszűrésére!
- Másolja be a jegyzőkönyvbe a Wireshark-ablak jellemző részletét vagy a teljes ablakot!
- Mentse el későbbi elemzés céljából a Wiresharkkal rögzített adatokat!
- Értelemszerűen ismételje meg a fentieket a többi célállomásra is!

2.1. Batch fájl szerkesztése

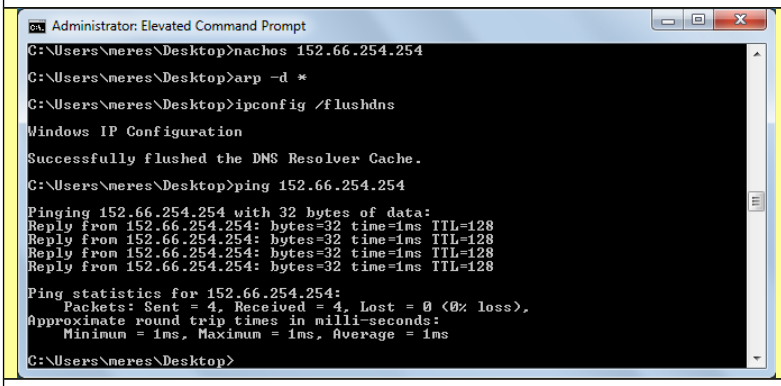
Készítsen egy batch fájlt, amely törli az ARP és DNS cache-t és kiadja a **`ping`** parancsot!

Másolja ide a fájl tartalmát!

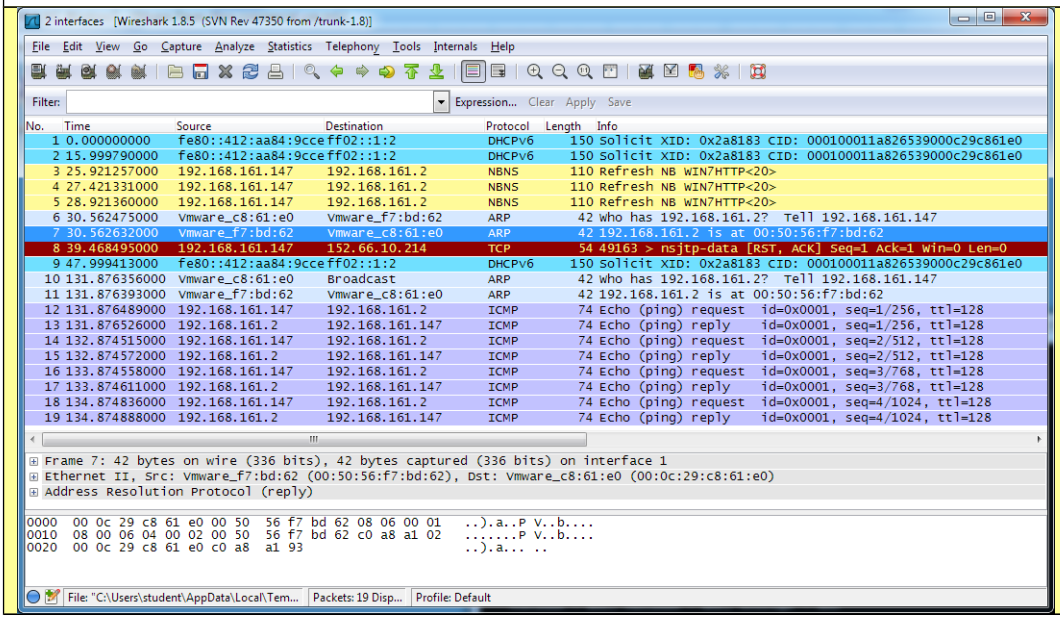
```
arp -d *
ipconfig /flushdns
ping %1
```

2.2. Alapértelmezett átjáró pingelése

Ping: alapértelmezett átjáró – cmd ablak képernyőképe

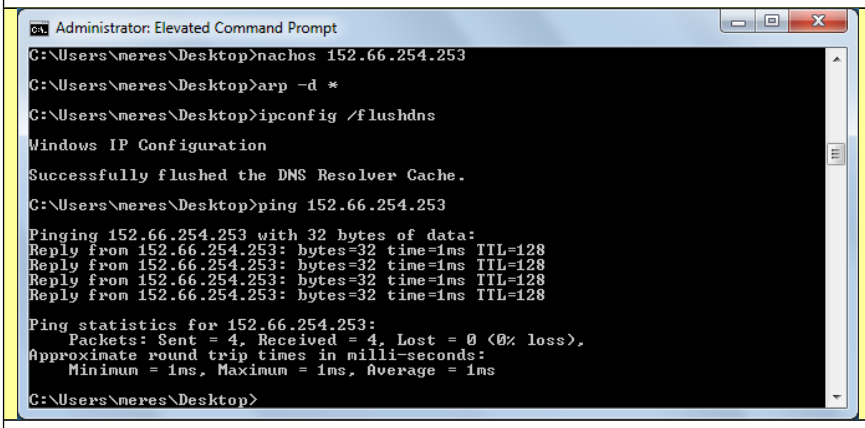


Ping: alapértelmezett átjáró – Wireshark forgalomrögzítés képernyőképe (szűrés nélkül)

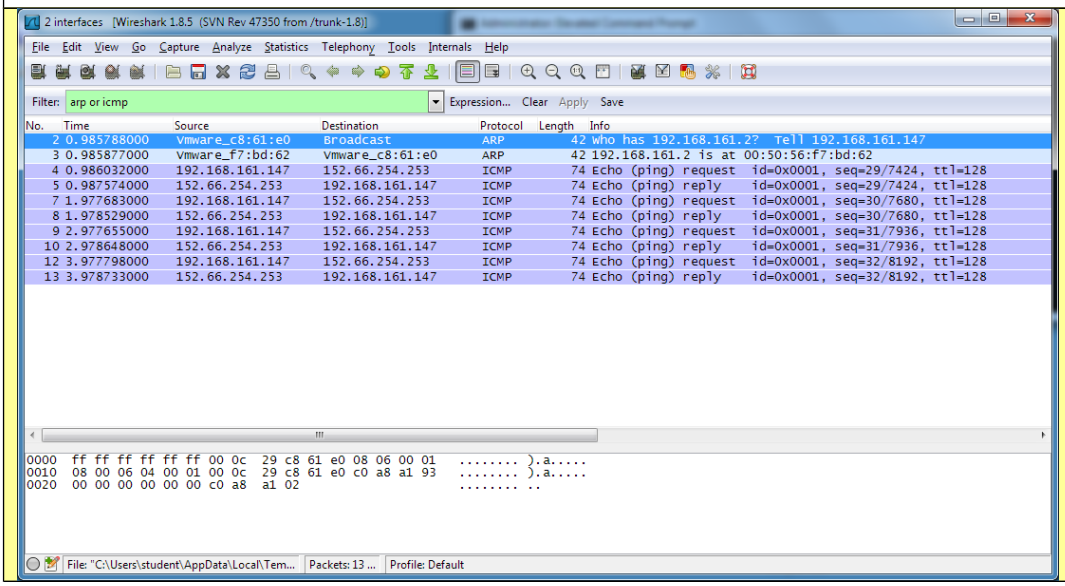


2.3. A labor DHCP szerverének pingelése

Ping: DHCP szerver – cmd ablak képernyőképe



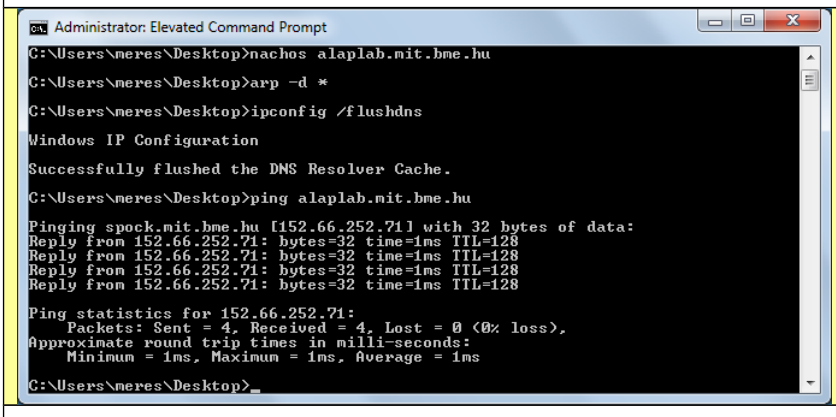
Ping: DHCP szerver – Wireshark forgalomrögzítés képernyőképe display filterrel



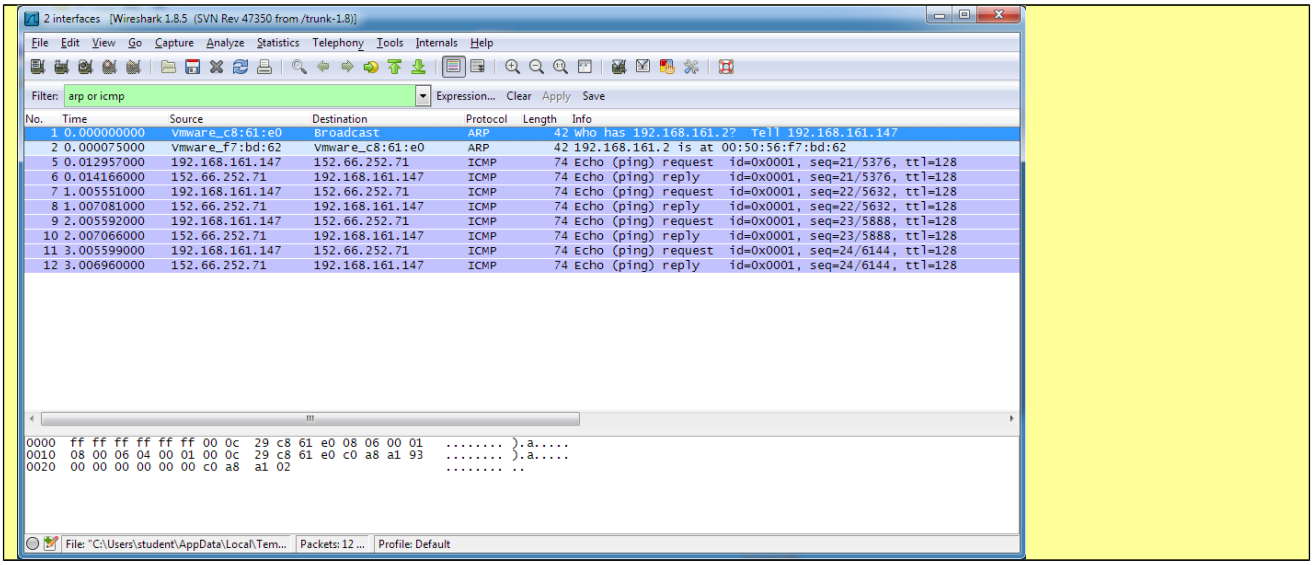
2.4. Az alaplabor szerverének pingelése

Ez valójában már nem az alaplabor szervere, de ez a mostani eredmény szempontjából mellékes.

Ping: alaplab.mit.bme.hu – cmd ablak képernyőképe

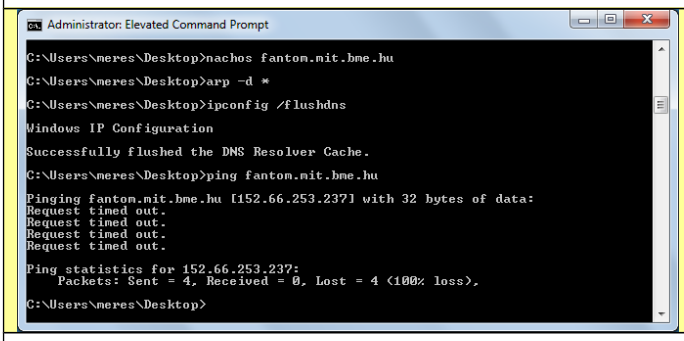


Ping: alaplab.mit.bme.hu – Wireshark forgalomrögzítés képernyőképe display filterrel

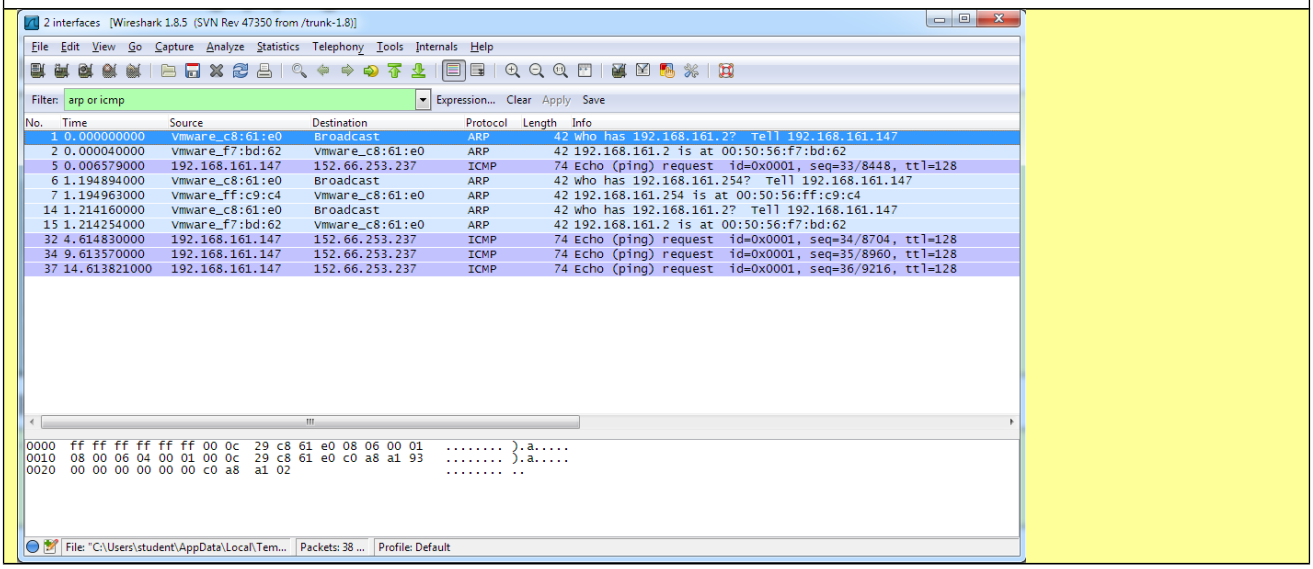


2.5. Fantom gép pingelése

Ping: fantom.mit.bme.hu – cmd ablak képernyőképe

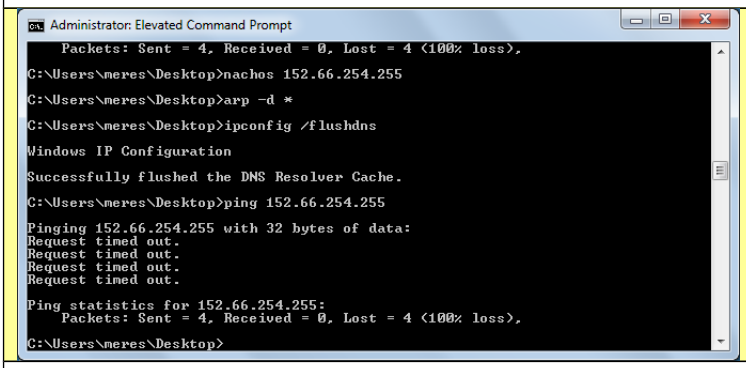


Ping: fantom.mit.bme.hu – Wireshark forgalomrögzítés képernyőképe display filterrel

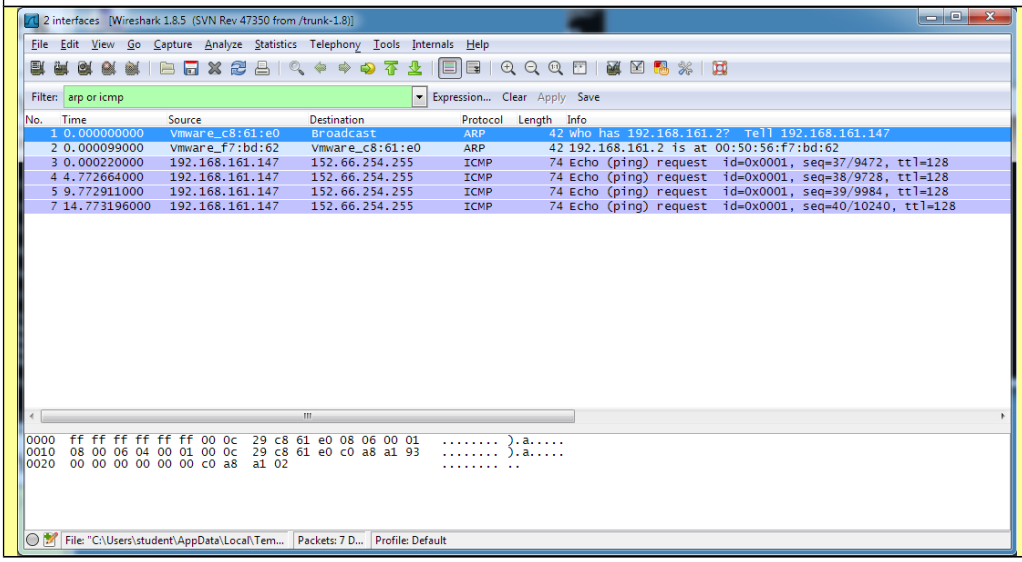


2.6. Subnet broadcast cím pingelése

Ping: subnet broadcast cím – cmd ablak képernyőképe



Ping: subnet broadcast cím – Wireshark forgalomrögzítés képernyőképe display filterrel



2.7. feladat

A következő esetekben sor került-e ARP és DNS kérésekre?

Ha igen, hány darabra, és mit kérdeztünk le? Ha nem, miért nem?

	ARP kérés(ek)	DNS kérés(ek)
Alapértelmezett átjáró:	1 db *(192.168.161.2)*	Nem
DHCP szerver:	1 db *(192.168.161.2)*	Nem
alaplab.mit.bme.hu:	1 db *(192.168.161.2)*	Igen

2.8. feladat

Milyen IP és Ethernet címeket használtunk a következő esetekben, és miért?		
	Cél Ethernet cím	Cél IP cím
Alapértelmezett átjáró	Cisco_f4:d4:00 (00:16:9c:f4:d4:00)	152.66.254.254
DHCP szerver	CadmusCo_6e:64:bf (08:00:27:6e:64:bf)	152.66.254.253
alaplab.mit.bme.hu	Cisco_f4:d4:00 (00:16:9c:f4:d4:00)	152.66.252.71
Indoklás: Az alapértelmezett átjárón fogja küldeni, mert ez kívül van a gateway-en.		

2.9. feladat

Hogyan kapcsolódik ez a mérés az előző feladatnál a **`route print`** parancsnál megismert kimeneti interfészválasztási megoldáshoz?
A routing táblázatot használja, amely a route print parancs kimenete. Interfészt választ és célcímet.

2.10. feladat

Az Ethernet címek alapján megállapítható az eszköz gyártója. Kik gyártották az egyes eszközöket? Mely eszközök gyártója nem ismerhető meg, és miért?	
	Gyártó
Saját gép	Gigabyte
Alapértelmezett átjáró:	Cisco
DHCP szerver:	Nem tudjuk megmondani, mert nem érhető el.
alaplab.mit.bme.hu	Nem tudjuk megmondani, mert nem érhető el.

2.11. feladat

Milyen címzést használ az ARP a kérésben és a válaszban, és miért?
Kéréshez: Broadcast, mert mindenkihez eljut. Válaszhoz: Unicast, mert csak a kérdezőhöz kell eljutnia.

2.12. feladat * (csak az ötösért)

Ehhez a két feladathoz a Wiresharkkal a fizikai hálózatra kapcsolódó interface-e kell figyelni. Azt a háttérforgalmat vizsgáljuk, amit az előző feladatoknál elkerültünk a virtuális hálózat használatával.

Milyen egyéb háttérforgalmat tapasztal a fizikai hálózaton? Ez miből származik?
Milyen protokoll az elsősorban háttérforgalomként megjelenő STP?
STP:
Milyen protokoll az elsősorban háttérforgalomként megjelenő LLDPP?
LLDP:
Milyen protokoll az elsősorban háttérforgalomként megjelenő SSDP?
SSDP:

2.13. Forgalomrögzítés capture filterrel * (csak az ötösért)

A forgalom jellemzőinek megfigyelése alapján konstruáljon capture filtert a zavaró SSDP és STP forgalom kiszűrésére!
Ping: ... – cmd ablak képernyőképe
<<cmd képernyőábra>>
Ping: ... – Wireshark forgalomrögzítés képernyőképe **capture** filterrel
<<Wireshark képernyőábra>>

3. feladat: A DNS működése

A feladat célja: a DNS működés alapjainak megismerése az **`nslookup`** program segítségével.

A kéréseket továbbra is a virtuális gépen adjuk ki, és a gazdagép megfelelő virtuális interface-ét figyeljük.

A mérés során csupán a domain névhez tartozó IP címet vagy egy adott IP címhez tartozó domain nevet határozunk meg az nslookup program segítségével.
Az nslookup futtatása előtt az előző méréshez hasonlóan törölje az ARP és DNS cache-t! Ennek a gyorsítására írjon batch file-et (mynslookup.bat)!

3.1. Batch fájl készítése: mynslookup

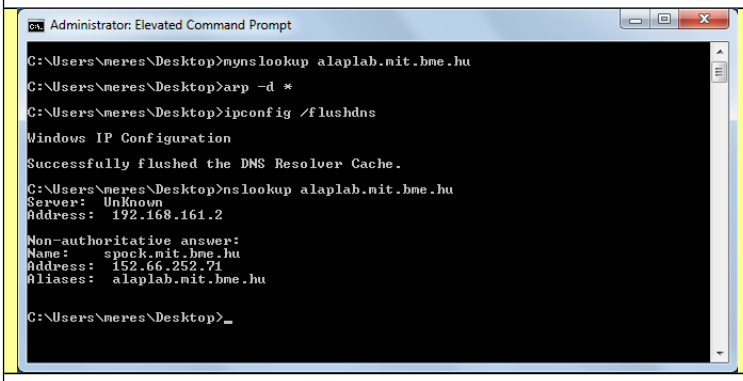
Adja meg a gyorsítótárak törlését, majd az **`nslookup`** meghívását elvégző batch fájl tartalmát!

```
arp -d *
ipconfig /flushdns
nslookup %1
```

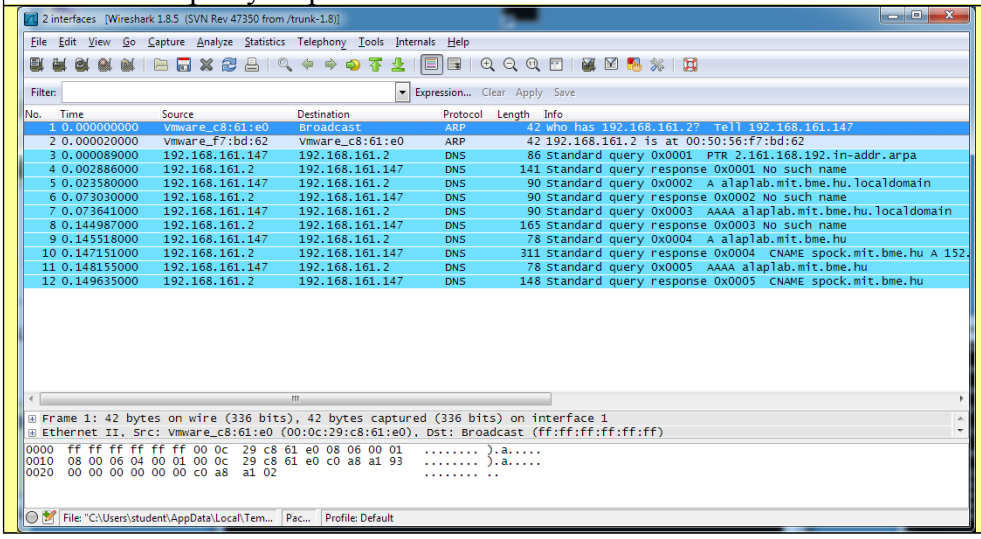
3.2. IP cím meghatározása domain név alapján 1.

Kérdezze le az alaplab.mit.bme.hu IP-címét a következő módon:

`mynslookup alaplab.mit.bme.hu`



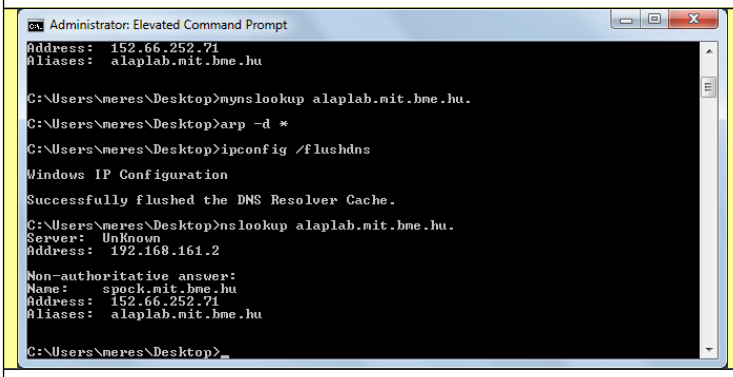
Wireshark képernyőkép



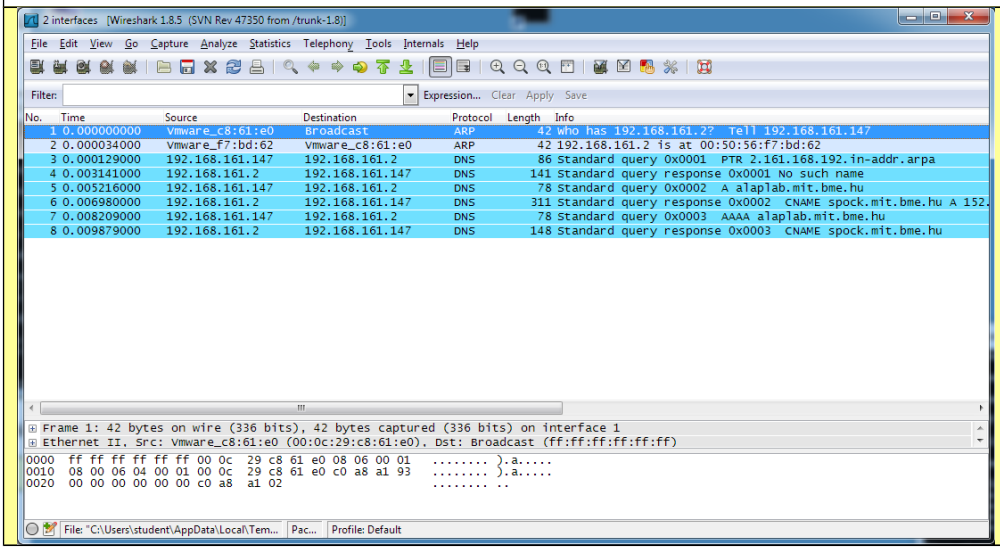
3.3. IP cím meghatározása domain név alapján 2.

Kérdezze le az alaplab.mit.bme.hu IP-címét a következő módon (ponttal a végén!):

```
mynslookup alaplab.mit.bme.hu.
```



Wireshark képernyőkép



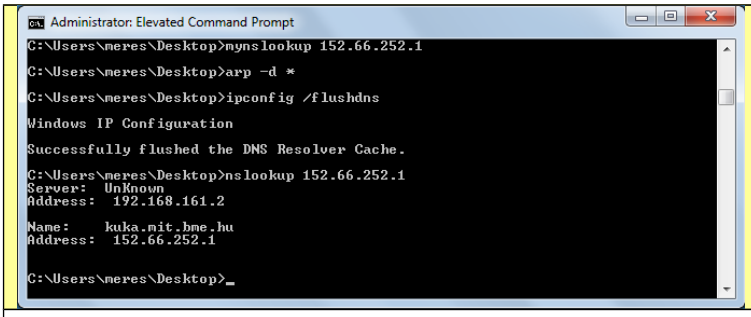
3.4. IP cím meghatározása domain név alapján: összehasonlítás

Mi a különbség a pont nélküli és a ponttal végződő lekérdezés között?

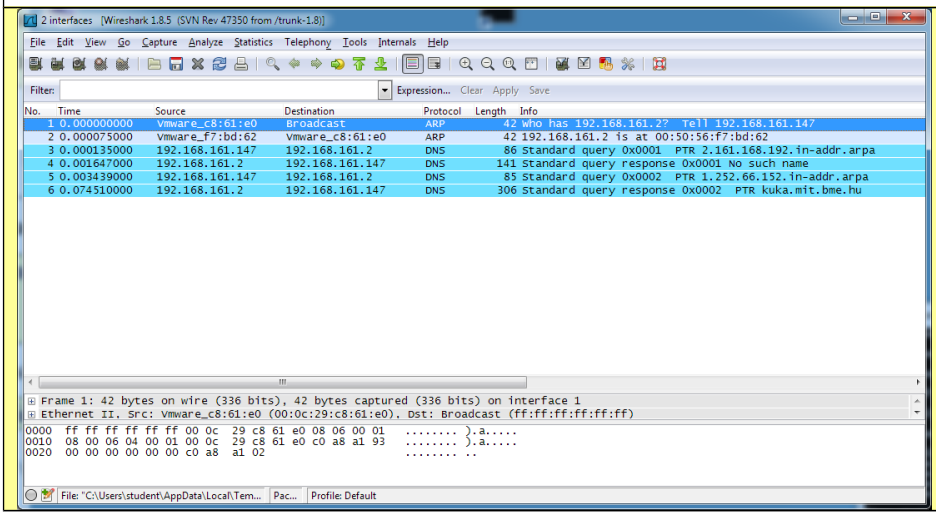
FQDN ponttal a végén és az ő IP címét kéri le. Pont nélkül DNS Suffix felhasználásával egészíti ki a címet.

3.5. Reverse lookup: domain név meghatározása IP cím alapján

Tudja meg a `152.66.252.1` IP című gép domain nevét (reverse lookup)!



Wireshark képernyőábra



3.6. A DNS működésének vizsgálata

Elemezze a Wireshark programmal a tapasztalt forgalmat az alábbiak szerint!
a) Hogyan történik meg az IP cím beállításokban megadott DNS Suffix Search List: **mit.bme.hu** beállítás felhasználása?
A DNS suffix-xal egészíti ki a megadott címet.
b) Milyen alacsonyabb szintű protokollokat használ a DNS, és hogyan?
UDP, IP, Ethernet
c) Hogyan történik az IP címek reprezentálása a DNS-ben reverse lookup esetén? Mi az IP cím mezőinek sorrendje, és miért?
Balról jobbra egyre szűkebb tartományt reprezentál, balról kezd.
d) Mit jelent a Time-To-Live paraméter a válaszban? Hogyan használják ezt fel? (**Figyelem**: ez kérdés a DNS kérésben visszaadott TTL-re vonatkozik, és nem az IP csomag TTL-jére!)
A DNS gyorstár kezeléséhez kell a TTL. Amikor a TTL=0 a DNS szerver frissíti a rekordot. A TTL értékéből debugolni lehet egy sikertelen elérés esetén.
e) Mi történik, ha egy adott domain névhez rendelt IP címet megváltoztatunk? Ki fogja elérni a

kérdéses gépet, és ki fog a régi IP című géphez fordulni?
A DNS szervereknek frissíteniük kell a táblájukat, hogy benne legyen az új IP. Ahol ez még nem történt meg vagy cacheben van a régi cím és nem frissítette, ott a régi IP címen fogják keresni.

3.7. feladat (csak az ötösért)*

Kérdezze le a **`www.cnn.com`** IP címét **`nslookup`**-pal!
<<cmd képernyőábra>>
<<Wireshark képernyőábra>>
Ismételje meg a **`www.cnn.com`** IP címének lekérdezését!
<<cmd képernyőábra>>
Wireshark képernyőábra
<<Wireshark képernyőábra>>
Hasonlítsa össze a kapott IP címeket! Mit tapasztalt? Miért hasznos a látott viselkedés? Vajon milyen két funkció ötvözésére használja ezt a CNN?

4. feladat: IP csomagok továbbításának útvonala

A feladat célja: útvonal-felderítés és nyomkövetés a **`tracert`** program segítségével.

Ezt a feladatot már a **fizikai gépen** végezze! Ügyeljen arra, hogy megfelelő hálózati interface-t figyeljen. Számítson a többi mérőpár forgalmának megjelenésére, használjon megjelenítési szűrőt.

A tracert egy olyan hálózati tesztprogram, amely a paraméterként megadott IP című vagy domain nevű gép és a tesztprogramot futtató gép között kísérletet tesz a köztes útvonalválasztók (routerek) meghatározására. (UNIX környezetben a traceroute vagy a tracepath látja el ugyanezt a feladatot. Tulajdonképpen ezek mintájára készült a tracert). A tracert futtatása előtt, az előző méréshez hasonlóan, törölje az ARP és DNS cache-t. Ennek a gyorsítására írjon batch file-et!

4.1. Batch fájl szerkesztése

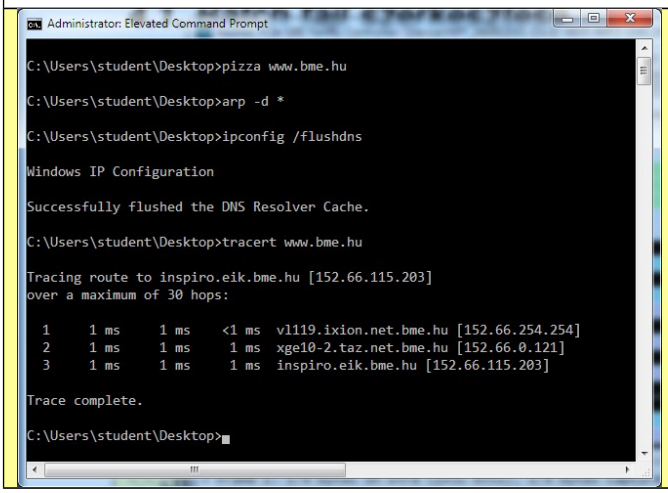
Készítsen egy batch fájlt, amely törli az ARP és DNS cache-t és kiadja a **`tracert`** parancsot!

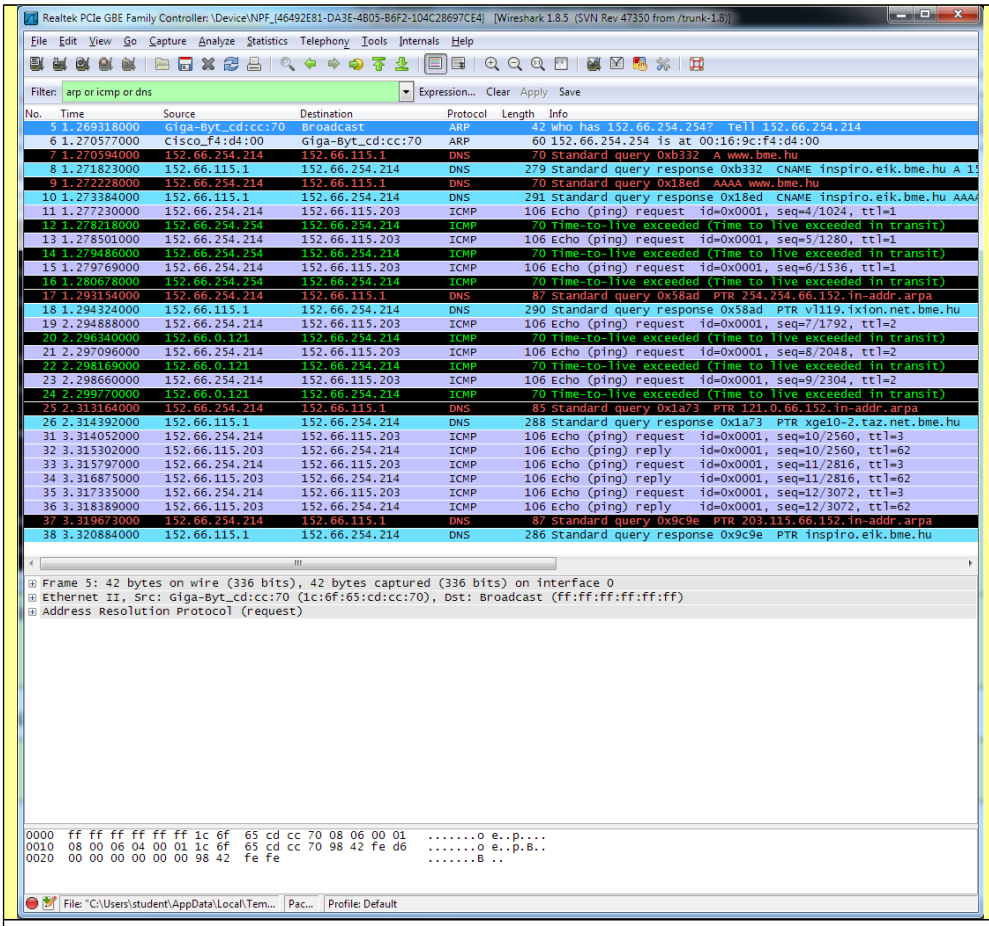
Másolja ide a fájl tartalmát!

```
arp -d *
ipconfig /flushdns
tracert %1
```

4.2. Nyomkövetés egy szerverig

A tracert paranccsal szólítsa meg a www.bme.hu szervert!



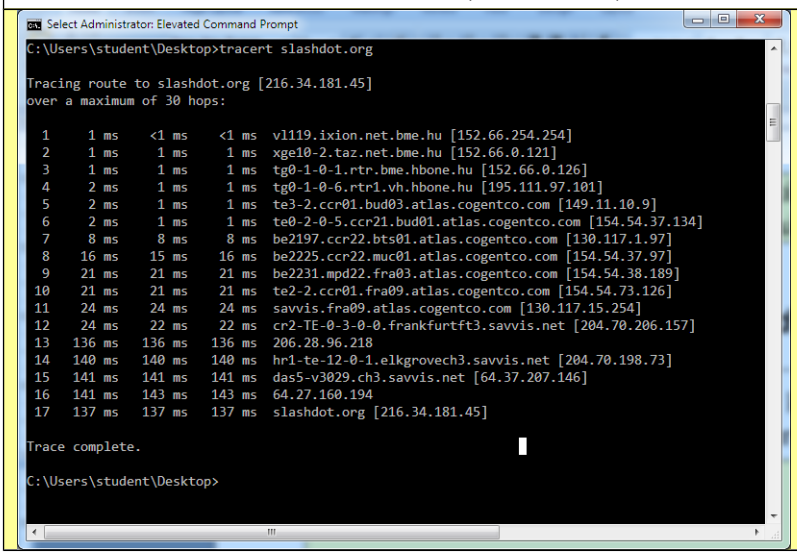


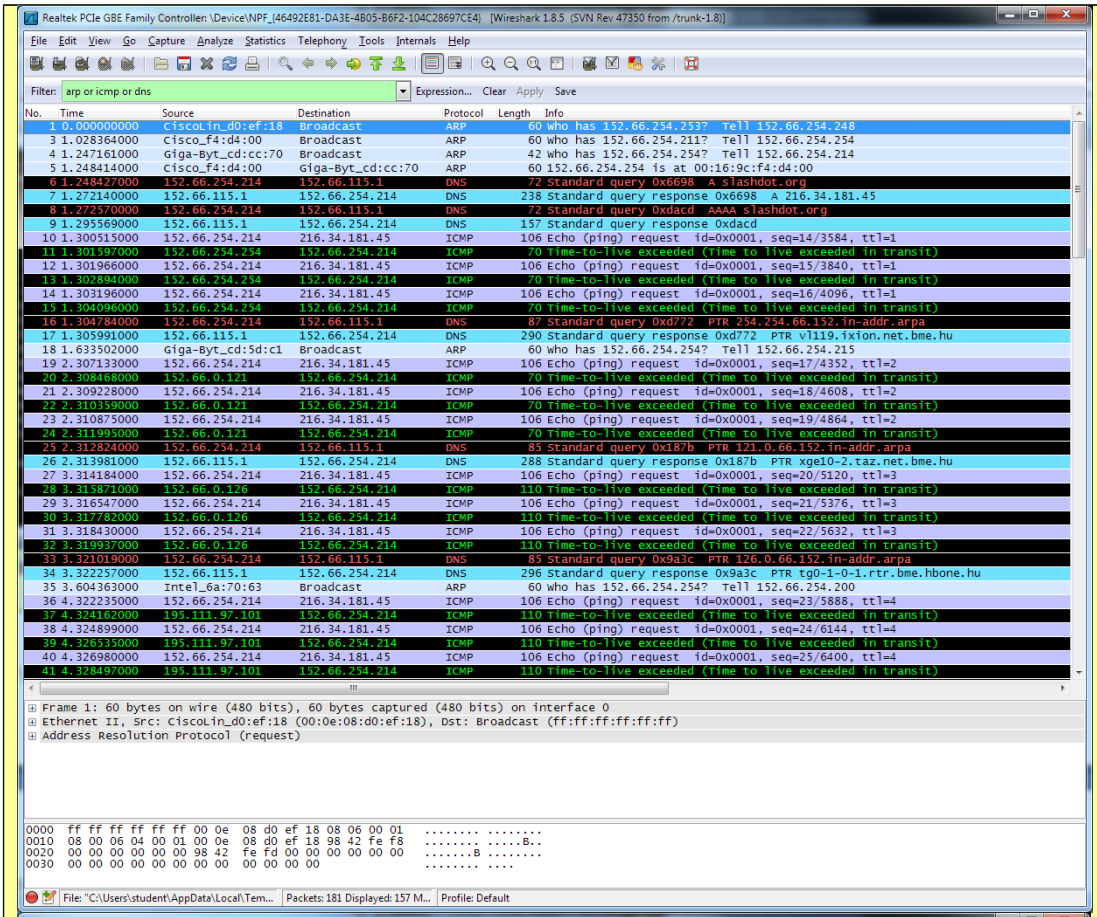
Elemezze a rögzített hálózati forgalmat.

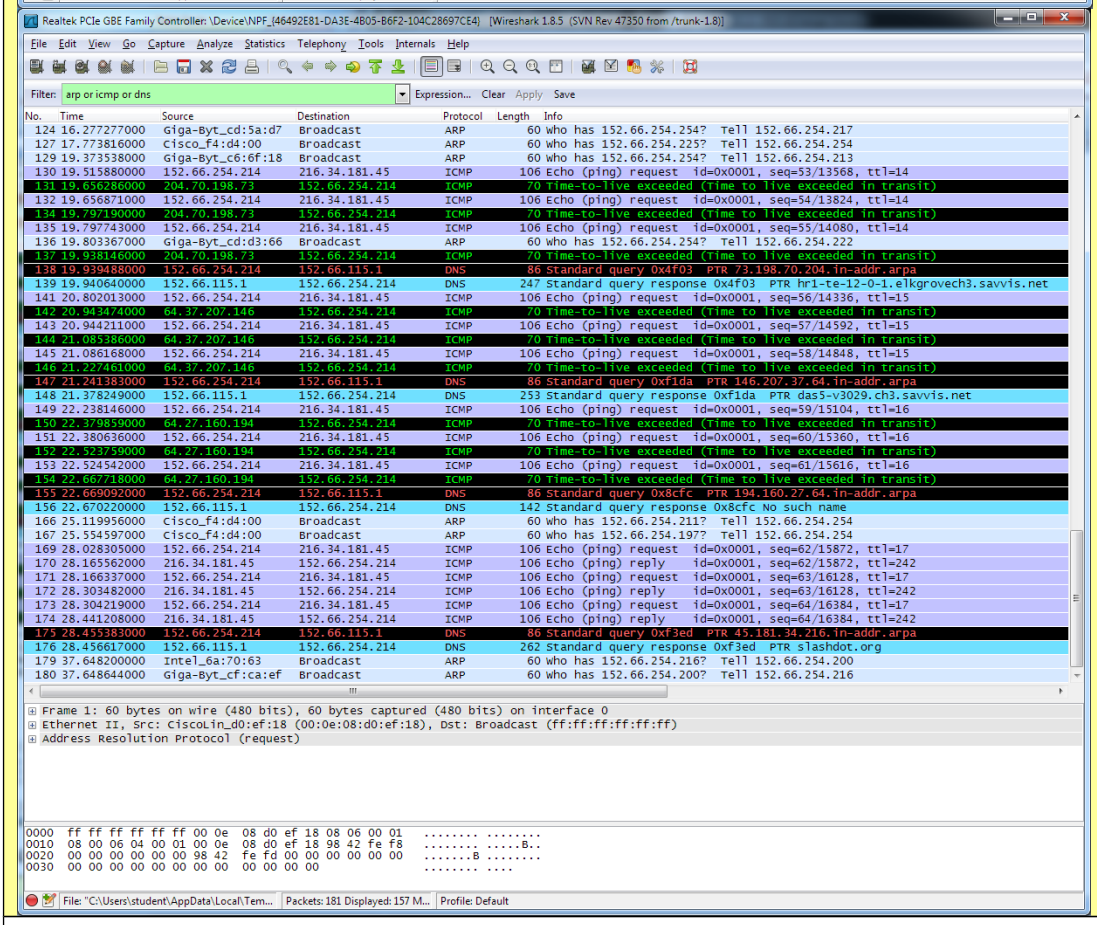
TTL=1,2,… ICMP csomagokkal kapjuk meg a pontokat, amelyeken átmegy a csomag.

4.3. Nyomkövetés egy külföldi szerverig 1.

A **tracert** paranccsal szólítson meg egy külföldi, lehetőleg tengerentúli (nagyszámú köztes útvonalválasztón keresztül elérhető) szervert! (Pl.: slashdot.org)





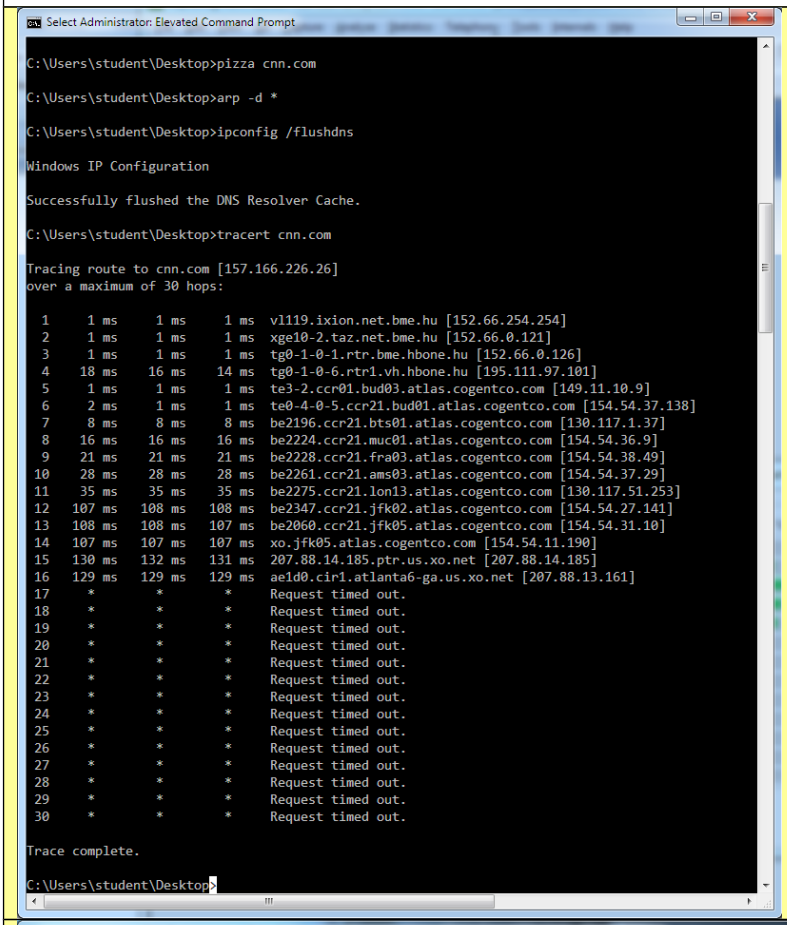


Elemezze a rögzített hálózati forgalmat!

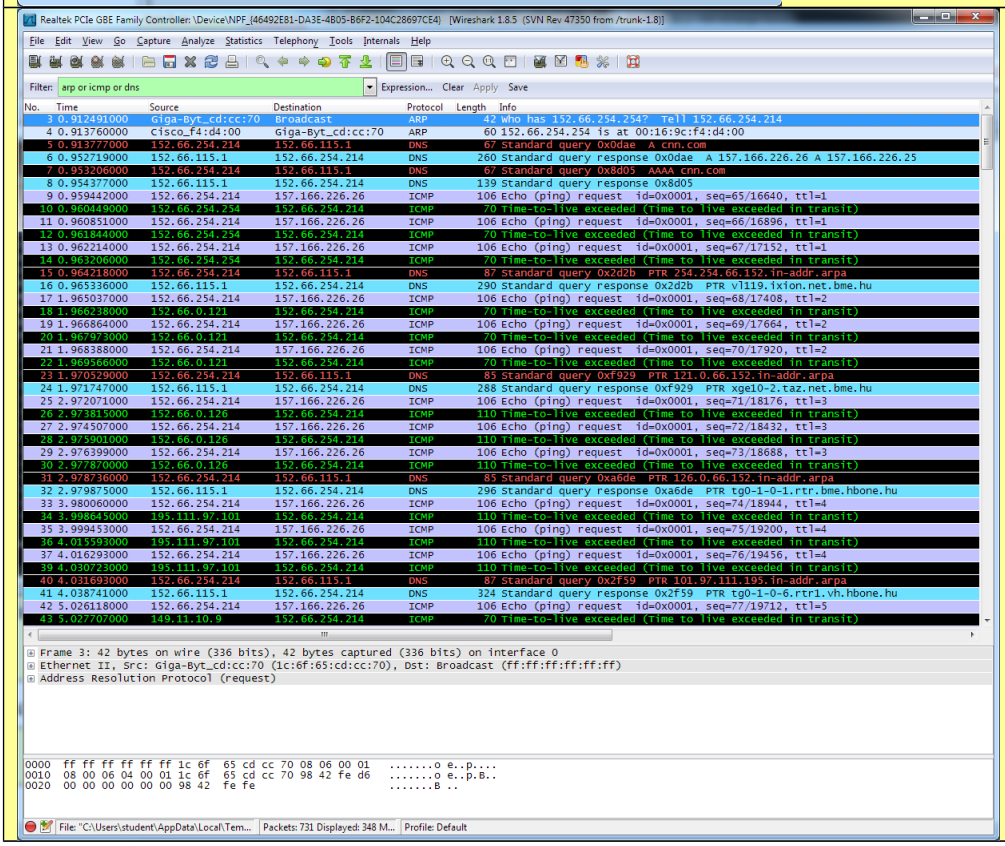
A nagyobb válaszidő jelzi, hogy távoli a link. Hosszabb utat tesz meg egy csomag.

4.4. Nyomkövetés egy külföldi szerverig 2.

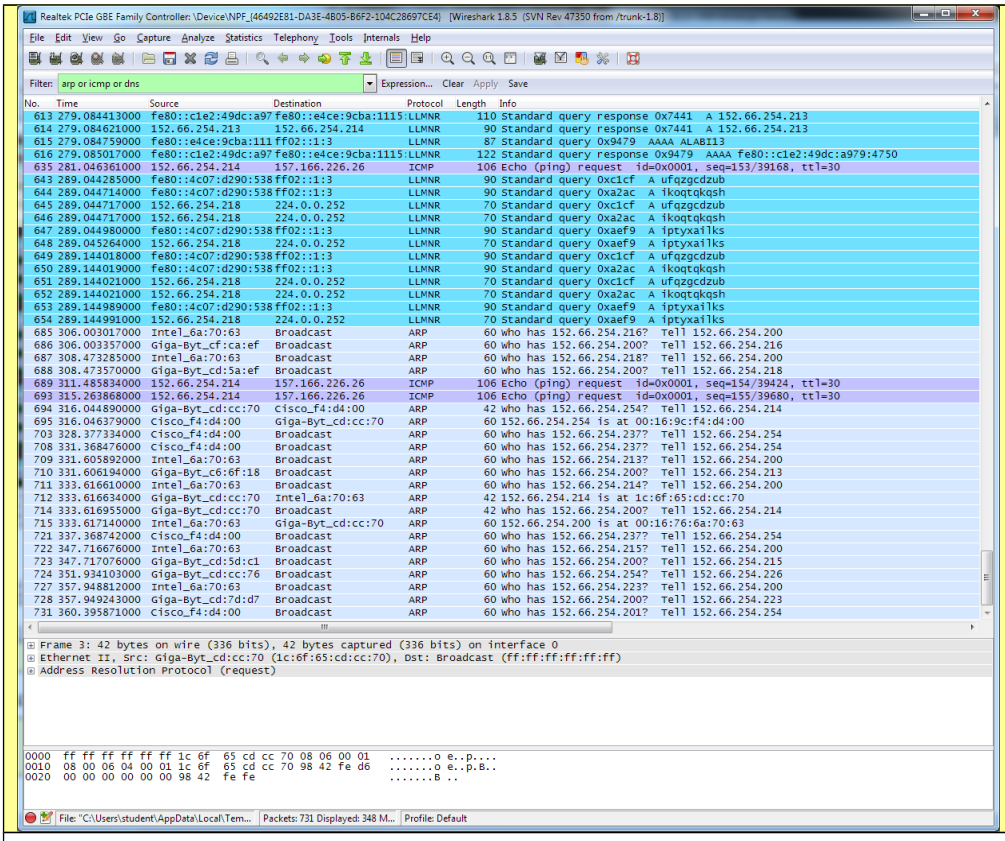
A **tracert** paranccsal szólítson meg egy külföldi, lehetőleg tengerentúli (nagyszámú köztes útvonalválasztón keresztül elérhető) szervert! (Pl.: cnn.com)



```
Select Administrator: Elevated Command Prompt

C:\Users\student\Desktop>pizza cnn.com

C:\Users\student\Desktop>arp -d *

C:\Users\student\Desktop>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\student\Desktop>tracert cnn.com

Tracing route to cnn.com [157.166.226.26]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  vl119.ixion.net.bme.hu [152.66.254.254]
  2     1 ms     1 ms     1 ms  xge10-2.taz.net.bme.hu [152.66.0.121]
  3     1 ms     1 ms     1 ms  tg0-1-0-1.rtr.bme.hbone.hu [152.66.0.126]
  4    18 ms    16 ms    14 ms  tg0-1-0-6.rtr1.vh.hbone.hu [195.111.97.101]
  5     1 ms     1 ms     1 ms  te3-2.ccr01.bud03.atlas.cogentco.com [149.11.10.9]
  6     2 ms     1 ms     1 ms  te0-4-0-5.ccr21.bud01.atlas.cogentco.com [154.54.37.138]
  7     8 ms     8 ms     8 ms  be2196.ccr21.bts01.atlas.cogentco.com [130.117.1.37]
  8    16 ms    16 ms    16 ms  be2224.ccr21.muc01.atlas.cogentco.com [154.54.36.9]
  9    21 ms    21 ms    21 ms  be2228.ccr21.fra03.atlas.cogentco.com [154.54.38.49]
 10    28 ms    28 ms    28 ms  be2261.ccr21.ams03.atlas.cogentco.com [154.54.37.29]
 11    35 ms    35 ms    35 ms  be2275.ccr21.lon13.atlas.cogentco.com [130.117.51.253]
 12   107 ms   108 ms   108 ms  be2347.ccr21.jfk02.atlas.cogentco.com [154.54.27.141]
 13   108 ms   108 ms   107 ms  be2060.ccr21.jfk05.atlas.cogentco.com [154.54.31.10]
 14   107 ms   107 ms   107 ms  xo.jfk05.atlas.cogentco.com [154.54.11.190]
 15   130 ms   132 ms   131 ms  207.88.14.185.ptr.us.xo.net [207.88.14.185]
 16   129 ms   129 ms   129 ms  ae1d0.cir1.atlanta6-ga.us.xo.net [207.88.13.161]
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

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



```
Realtek PCIe GBE Family Controller: \Device\NPF_{46492E81-DA3E-4B05-B6F2-104C28697CE4}  [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Tools  Internals  Help
Filter: arp or icmp or dns   Expression...  Clear  Apply  Save

No.  Time        Source              Destination         Protocol  Length  Info
  3  0.912491000  Giga-Byt_cd:cc:70   Broadcast           ARP         42  Who has 152.66.254.254?  Tell 152.66.254.214
  4  0.913760000  Cisco_f4:d4:00      Giga-Byt_cd:cc:70   ARP         60  152.66.254.254 is at 00:16:9c:f4:d4:00
  5  0.913777000  152.66.254.214      152.66.115.1        DNS         67  Standard query 0x0dae  A cnn.com
  6  0.952719000  152.66.115.1        152.66.254.214      DNS        260  Standard query response 0x0dae  A 157.166.226.26 A 157.166.226.25
  7  0.953206000  152.66.254.214      152.66.115.1        DNS         67  Standard query 0x8d05  AAAA cnn.com
  8  0.954377000  152.66.115.1        152.66.254.214      DNS        139  Standard query response 0x8d05
  9  0.959442000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=65/16640, ttl=1
 10  0.960449000  152.66.254.254      152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
 11  0.960851000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=66/16896, ttl=1
 12  0.961844000  152.66.254.254      152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
 13  0.962214000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=67/17152, ttl=1
 14  0.963206000  152.66.254.254      152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
 15  0.964218000  152.66.254.214      152.66.115.1        DNS         87  Standard query 0x2d2b  PTR 254.254.66.152.in-addr.arpa
 16  0.965336000  152.66.115.1        152.66.254.214      DNS        290  Standard query response 0x2d2b  PTR vl119.ixion.net.bme.hu
 17  1.965037000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=68/17408, ttl=2
 18  1.966238000  152.66.0.121        152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
 19  1.966864000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=69/17664, ttl=2
 20  1.967373000  152.66.0.121        152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
 21  1.968388000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=70/17920, ttl=2
 22  1.969366000  152.66.0.121        152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)
 23  1.970529000  152.66.254.214      152.66.115.1        DNS         85  Standard query 0xf929  PTR 121.0.66.152.in-addr.arpa
 24  1.971747000  152.66.115.1        152.66.254.214      DNS        288  Standard query response 0xf929  PTR xge10-2.taz.net.bme.hu
 25  2.972071000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=71/18176, ttl=3
 26  2.973815000  152.66.0.126        152.66.254.214      ICMP        110 Time-to-live exceeded (Time to live exceeded in transit)
 27  2.974507000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=72/18432, ttl=3
 28  2.975901000  152.66.0.126        152.66.254.214      ICMP        110 Time-to-live exceeded (Time to live exceeded in transit)
 29  2.976399000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=73/18688, ttl=3
 30  2.977870000  152.66.0.126        152.66.254.214      ICMP        110 Time-to-live exceeded (Time to live exceeded in transit)
 31  2.978736000  152.66.254.214      152.66.115.1        DNS         85  Standard query 0xa6de  PTR 126.0.66.152.in-addr.arpa
 32  2.979875000  152.66.115.1        152.66.254.214      DNS        296  Standard query response 0xa6de  PTR tg0-1-0-1.rtr.bme.hbone.hu
 33  3.980060000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=74/18944, ttl=4
 34  3.998645000  195.111.97.101      152.66.254.214      ICMP        110 Time-to-live exceeded (Time to live exceeded in transit)
 35  3.999453000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=75/19200, ttl=4
 36  4.015593000  195.111.97.101      152.66.254.214      ICMP        110 Time-to-live exceeded (Time to live exceeded in transit)
 37  4.016293000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=76/19456, ttl=4
 39  4.030723000  195.111.97.101      152.66.254.214      ICMP        110 Time-to-live exceeded (Time to live exceeded in transit)
 40  4.031693000  152.66.254.214      152.66.115.1        DNS         87  Standard query 0x2f59  PTR 101.97.111.195.in-addr.arpa
 41  4.038741000  152.66.115.1        152.66.254.214      DNS        324  Standard query response 0x2f59  PTR tg0-1-0-6.rtr1.vh.hbone.hu
 42  5.026118000  152.66.254.214      157.166.226.26      ICMP       106  Echo (ping) request  id=0x0001, seq=77/19712, ttl=5
 43  5.027707000  149.11.10.9         152.66.254.214      ICMP        70  Time-to-live exceeded (Time to live exceeded in transit)

Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Giga-Byt_cd:cc:70 (1c:6f:65:cd:cc:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 1c 6f  65 cd cc 70 08 06 00 01   .......o e..p....
0010  08 00 06 04 00 01 1c 6f  65 cd cc 70 98 42 fe d6   .......o e..p.B..
0020  00 00 00 00 00 00 98 42  fe fe                     .......B ..

File: "C:\Users\student\AppData\Local\Tem...  Packets: 731 Displayed: 348 M...  Profile: Default
```



Elemezze a rögzített hálózati forgalmat!

Blokkolták a kérést, mert a 17. hoptól nem tudja feloldani a címeket.

4.5. A `tracert` működése

Hogyan működik a tracert parancs, hogyan határozza meg a köztes útvonalválasztókat? Milyen protokollokat használ, és hogyan?

Egyre nagyobb TTL értékű ICMP csomagokkal deríti fel a hálózatot. Közben ARP segítségével végez címfeloldást.

4.6. feladat * (csak az ötösért)

Mi történik, ha a **tracert** paranccsal megszólított gép ki van kapcsolva vagy a rajta konfigurált tűzfal tiltja a program által küldött csomagokra történő választ? Produkálja a jelenséget!

<<cmd képernyőábra>>

<<Wireshark képernyőábra>>

Magyarázat:

5. feladat: TCP adatfolyamok vizsgálata a netstat programmal

A feladat célja: TCP adatfolyamok vizsgálata a **`netstat`** és a Wireshark programmal.

Ez a mérés akár a virtuális, akár a fizikai gépen is elvégezhető. Ügyeljen arra, hogy megfelelő hálózati interface-t figyeljen.

A mérés során egy webböngészővel le kell tölteni egy honlapot, és az így kialakuló forgalmat kell vizsgálni a megfelelő időközökben futtatott a **`netstat`** programmal. A webböngészők a letöltött tartalmat cache-elik. A cache és a HTTP protokoll vizsgálata a következő laborfoglalkozás témája lesz, most csupán azt kell elérni, hogy a teljes weblap letöltődjön.

A mérés során az alábbi részfeladatokat kell elvégezni:

- Futtassa le a **`netstat-a`** parancsot! A kimenetet tárolja el egy file-ba (pl. netstat_pre.txt)!
- Indítsa le a webböngészőt, és törölje a böngésző cache-ét!
- Törölje az ARP és DNS cache-t!
- Indítsa el a forgalomrögzítést!
- Töltse le a **`www.bme.hu`** weblapot!
- Futtassa le a **`netstat-a`** parancsot! A kimenetet tárolja el egy file-ba (pl. netstat_web.txt)!
- Lépjen ki a böngészőből!
- Futtassa le a **`netstat-a`** parancsot, a kimenetet tárolja el egy file-ba (pl. netstat_post.txt)!
- Állítsa le a forgalomrögzítést!

5.1. feladat: „pre”

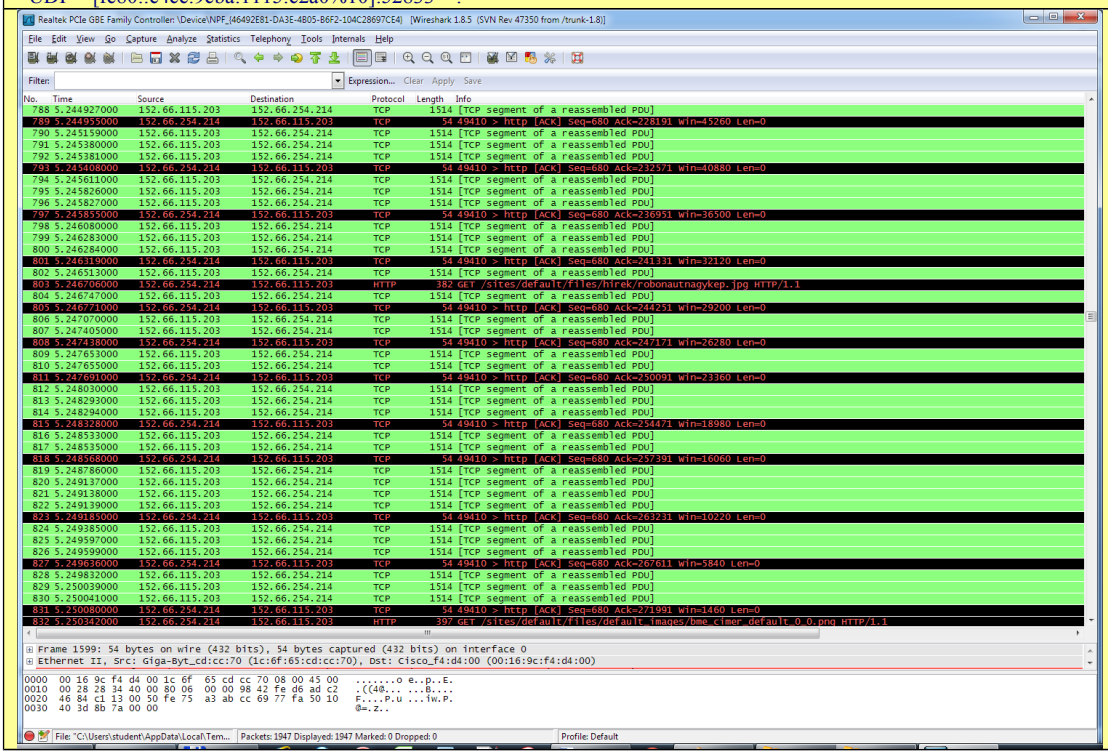
```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            alabi14:0              LISTENING
  TCP    0.0.0.0:445            alabi14:0              LISTENING
  TCP    0.0.0.0:902            alabi14:0              LISTENING
  TCP    0.0.0.0:912            alabi14:0              LISTENING
  TCP    0.0.0.0:49152          alabi14:0              LISTENING
  TCP    0.0.0.0:49153          alabi14:0              LISTENING
  TCP    0.0.0.0:49154          alabi14:0              LISTENING
  TCP    0.0.0.0:49156          alabi14:0              LISTENING
  TCP    0.0.0.0:49170          alabi14:0              LISTENING
  TCP    127.0.0.1:12080        alabi14:0              LISTENING
  TCP    127.0.0.1:27275        alabi14:0              LISTENING
  TCP    127.0.0.1:49323        alabi14:49324          ESTABLISHED
  TCP    127.0.0.1:49324        alabi14:49323          ESTABLISHED
  TCP    127.0.0.1:49325        alabi14:49326          ESTABLISHED
  TCP    127.0.0.1:49326        alabi14:49325          ESTABLISHED
  TCP    152.66.254.214:139     alabi14:0              LISTENING
  TCP    152.66.254.214:49158   r-052-042-234-077:http  ESTABLISHED
  TCP    152.66.254.214:49247   a345vg:https           CLOSE_WAIT
  TCP    152.66.254.214:49248   fra07s31-in-f30:https  CLOSE_WAIT
  TCP    152.66.254.214:49249   fra07s31-in-f30:https  CLOSE_WAIT
  TCP    152.66.254.214:49250   a92-123-150-13:https   CLOSE_WAIT
  TCP    152.66.254.214:49251   a92-123-150-13:https   CLOSE_WAIT
  TCP    152.66.254.214:49277   fileshare:microsoft-ds  ESTABLISHED
  TCP    192.168.161.1:139      alabi14:0              LISTENING
  TCP    192.168.241.1:139      alabi14:0              LISTENING
  TCP    [::]:135               alabi14:0              LISTENING
  TCP    [::]:445               alabi14:0              LISTENING
  TCP    [::]:49152             alabi14:0              LISTENING
  TCP    [::]:49153             alabi14:0              LISTENING
  TCP    [::]:49154             alabi14:0              LISTENING
  TCP    [::]:49156             alabi14:0              LISTENING
  TCP    [::]:49170             alabi14:0              LISTENING
  UDP    0.0.0.0:5355           *:*
```

```
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:52836        *:*
  UDP    152.66.254.214:137     *:*
  UDP    152.66.254.214:138     *:*
  UDP    152.66.254.214:1900    *:*
  UDP    152.66.254.214:52835   *:*
  UDP    192.168.161.1:137      *:*
  UDP    192.168.161.1:138      *:*
  UDP    192.168.161.1:1900     *:*
  UDP    192.168.241.1:137      *:*
  UDP    192.168.241.1:138      *:*
  UDP    192.168.241.1:1900     *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:52834            *:*
  UDP    [fe80::283c:5163:e772:ed42%17]:546  *:*
  UDP    [fe80::283c:5163:e772:ed42%17]:1900  *:*
  UDP    [fe80::2961:5c10:eb86:427%15]:546  *:*
  UDP    [fe80::2961:5c10:eb86:427%15]:1900  *:*
  UDP    [fe80::e4ce:9cba:1115:c2a0%10]:546  *:*
  UDP    [fe80::e4ce:9cba:1115:c2a0%10]:1900  *:*
  UDP    [fe80::e4ce:9cba:1115:c2a0%10]:52833  *:*
```

5.2. feladat: „web”

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            alabi14:0              LISTENING
  TCP    0.0.0.0:445            alabi14:0              LISTENING
  TCP    0.0.0.0:902            alabi14:0              LISTENING
  TCP    0.0.0.0:912            alabi14:0              LISTENING
  TCP    0.0.0.0:49152          alabi14:0              LISTENING
  TCP    0.0.0.0:49153          alabi14:0              LISTENING
  TCP    0.0.0.0:49154          alabi14:0              LISTENING
  TCP    0.0.0.0:49156          alabi14:0              LISTENING
  TCP    0.0.0.0:49170          alabi14:0              LISTENING
  TCP    127.0.0.1:12080        alabi14:0              LISTENING
  TCP    127.0.0.1:12080        alabi14:49405          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49407          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49408          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49409          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49411          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49412          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49417          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49418          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49422          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49423          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49424          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49426          ESTABLISHED
  TCP    127.0.0.1:12080        alabi14:49429          ESTABLISHED
  TCP    127.0.0.1:27275        alabi14:0              LISTENING
  TCP    127.0.0.1:49323        alabi14:49324          ESTABLISHED
  TCP    127.0.0.1:49324        alabi14:49323          ESTABLISHED
  TCP    127.0.0.1:49325        alabi14:49326          ESTABLISHED
  TCP    127.0.0.1:49326        alabi14:49325          ESTABLISHED
  TCP    127.0.0.1:49374        alabi14:49375          ESTABLISHED
  TCP    127.0.0.1:49375        alabi14:49374          ESTABLISHED
  TCP    127.0.0.1:49405        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49407        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49408        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49409        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49411        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49412        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49417        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49418        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49422        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49423        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49424        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49426        alabi14:12080          ESTABLISHED
  TCP    127.0.0.1:49429        alabi14:12080          ESTABLISHED
  TCP    152.66.254.214:139     alabi14:0              LISTENING
  TCP    152.66.254.214:49158   r-052-042-234-077:http  ESTABLISHED
  TCP    152.66.254.214:49247   a345vg:https           CLOSE_WAIT
  TCP    152.66.254.214:49248   fra07s31-in-f30:https  CLOSE_WAIT
  TCP    152.66.254.214:49249   fra07s31-in-f30:https  CLOSE_WAIT
```

```
TCP    152.66.254.214:49250   a92-123-150-13:https   CLOSE_WAIT
TCP    152.66.254.214:49251   a92-123-150-13:https   CLOSE_WAIT
TCP    152.66.254.214:49277   fileshare:microsoft-ds  ESTABLISHED
TCP    152.66.254.214:49394   fa-in-f101:http        TIME_WAIT
TCP    152.66.254.214:49395   fa-in-f101:http        TIME_WAIT
TCP    152.66.254.214:49406   inspiro:http           ESTABLISHED
TCP    152.66.254.214:49410   inspiro:http           ESTABLISHED
TCP    152.66.254.214:49413   inspiro:http           ESTABLISHED
TCP    152.66.254.214:49414   inspiro:http           ESTABLISHED
TCP    152.66.254.214:49415   inspiro:http           ESTABLISHED
TCP    152.66.254.214:49416   inspiro:http           ESTABLISHED
TCP    152.66.254.214:49419   fa-in-f95:http         ESTABLISHED
TCP    152.66.254.214:49420   fa-in-f95:http         ESTABLISHED
TCP    152.66.254.214:49425   fa-in-f132:http        ESTABLISHED
TCP    152.66.254.214:49427   fa-in-f132:http        ESTABLISHED
TCP    152.66.254.214:49428   fa-in-f132:http        ESTABLISHED
TCP    152.66.254.214:49430   fa-in-f132:http        ESTABLISHED
TCP    152.66.254.214:49431   fa-in-f132:http        ESTABLISHED
TCP    192.168.161.1:139      alabi14:0              LISTENING
TCP    192.168.241.1:139      alabi14:0              LISTENING
TCP    [::]:135               alabi14:0              LISTENING
TCP    [::]:445               alabi14:0              LISTENING
TCP    [::]:49152             alabi14:0              LISTENING
TCP    [::]:49153             alabi14:0              LISTENING
TCP    [::]:49154             alabi14:0              LISTENING
TCP    [::]:49156             alabi14:0              LISTENING
TCP    [::]:49170             alabi14:0              LISTENING
UDP    0.0.0.0:5355           *:*
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:52836        *:*
UDP    152.66.254.214:137     *:*
UDP    152.66.254.214:138     *:*
UDP    152.66.254.214:1900    *:*
UDP    152.66.254.214:52835   *:*
UDP    192.168.161.1:137      *:*
UDP    192.168.161.1:138      *:*
UDP    192.168.161.1:1900     *:*
UDP    192.168.241.1:137      *:*
UDP    192.168.241.1:138      *:*
UDP    192.168.241.1:1900     *:*
UDP    [::]:5355              *:*
UDP    [::1]:1900             *:*
UDP    [::1]:52834            *:*
UDP    [fe80::283c:5163:e772:ed42%17]:1900  *:*
UDP    [fe80::2961:5c10:eb86:427%15]:1900  *:*
UDP    [fe80::e4ce:9cba:1115:c2a0%10]:1900  *:*
UDP    [fe80::e4ce:9cba:1115:c2a0%10]:52833  *:*
```



5.3. feladat: „post”

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            alabi14:0              LISTENING
  TCP    0.0.0.0:445            alabi14:0              LISTENING
  TCP    0.0.0.0:902            alabi14:0              LISTENING
  TCP    0.0.0.0:912            alabi14:0              LISTENING
  TCP    0.0.0.0:49152          alabi14:0              LISTENING
  TCP    0.0.0.0:49153          alabi14:0              LISTENING
  TCP    0.0.0.0:49154          alabi14:0              LISTENING
  TCP    0.0.0.0:49156          alabi14:0              LISTENING
  TCP    0.0.0.0:49170          alabi14:0              LISTENING
  TCP    127.0.0.1:12080        alabi14:0              LISTENING
  TCP    127.0.0.1:27275        alabi14:0              LISTENING
  TCP    127.0.0.1:49323        alabi14:49324          ESTABLISHED
  TCP    127.0.0.1:49324        alabi14:49323          ESTABLISHED
  TCP    127.0.0.1:49325        alabi14:49326          ESTABLISHED
  TCP    127.0.0.1:49326        alabi14:49325          ESTABLISHED
  TCP    127.0.0.1:49375        alabi14:49374          TIME_WAIT
  TCP    152.66.254.214:139     alabi14:0              LISTENING
  TCP    152.66.254.214:49158   r-052-042-234-077:http  ESTABLISHED
  TCP    152.66.254.214:49247   a345vg:https           CLOSE_WAIT
  TCP    152.66.254.214:49248   fra07s31-in-f30:https  CLOSE_WAIT
  TCP    152.66.254.214:49249   fra07s31-in-f30:https  CLOSE_WAIT
  TCP    152.66.254.214:49250   a92-123-150-13:https   CLOSE_WAIT
  TCP    152.66.254.214:49251   a92-123-150-13:https   CLOSE_WAIT
  TCP    152.66.254.214:49277   fileshare:microsoft-ds  ESTABLISHED
  TCP    152.66.254.214:49394   fa-in-f101:http        TIME_WAIT
  TCP    152.66.254.214:49395   fa-in-f101:http        TIME_WAIT
  TCP    152.66.254.214:49419   fa-in-f95:http         TIME_WAIT
  TCP    152.66.254.214:49420   fa-in-f95:http         TIME_WAIT
  TCP    152.66.254.214:49425   fa-in-f132:http        TIME_WAIT
  TCP    152.66.254.214:49427   fa-in-f132:http        TIME_WAIT
  TCP    152.66.254.214:49428   fa-in-f132:http        TIME_WAIT
  TCP    152.66.254.214:49430   fa-in-f132:http        TIME_WAIT
  TCP    152.66.254.214:49431   fa-in-f132:http        TIME_WAIT
  TCP    192.168.161.1:139      alabi14:0              LISTENING
  TCP    192.168.241.1:139      alabi14:0              LISTENING
  TCP    [::]:135               alabi14:0              LISTENING
  TCP    [::]:445               alabi14:0              LISTENING
  TCP    [::]:49152             alabi14:0              LISTENING
  TCP    [::]:49153             alabi14:0              LISTENING
  TCP    [::]:49154             alabi14:0              LISTENING
  TCP    [::]:49156             alabi14:0              LISTENING
  TCP    [::]:49170             alabi14:0              LISTENING
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:52836        *:*
  UDP    152.66.254.214:137     *:*
  UDP    152.66.254.214:138     *:*
  UDP    152.66.254.214:1900    *:*
  UDP    152.66.254.214:52835   *:*
  UDP    192.168.161.1:137      *:*
  UDP    192.168.161.1:138      *:*
  UDP    192.168.161.1:1900     *:*
  UDP    192.168.241.1:137      *:*
  UDP    192.168.241.1:138      *:*
  UDP    192.168.241.1:1900     *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:52834            *:*
  UDP    [fe80::283c:5163:e772:ed42%17]:1900  *:*
  UDP    [fe80::2961:5c10:eb86:427%15]:1900  *:*
  UDP    [fe80::e4ce:9cba:1115:c2a0%10]:1900  *:*
  UDP    [fe80::e4ce:9cba:1115:c2a0%10]:52833  *:*
```

5.4. A letöltéskor használt protokoll azonosítása

Milyen protokollokat használ a webböngésző a tartalom letöltése során, és milyen célból?
HTTP – alkalmazási rétegbeli protokoll, a weblapot leíró adatok érkeznek vele

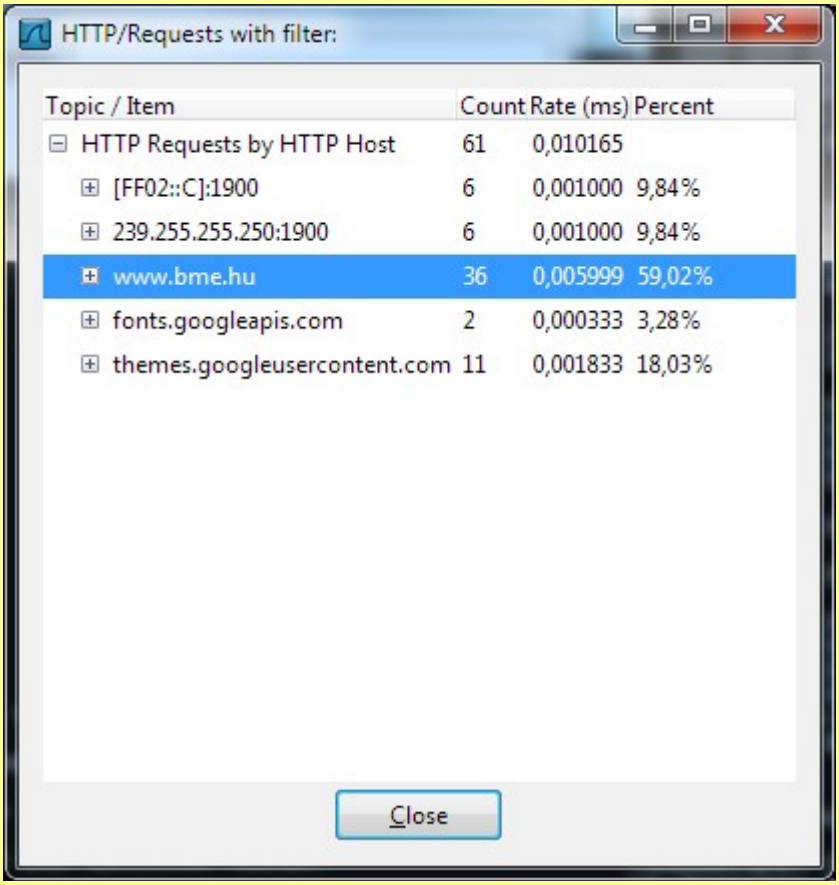
TCP – szállítási rétegbeli protokoll, a weblaphoz kapcsolódó adatok (képek, js) érkeznek rajta

5.5. A TCP folyamok számának meghatározása

A mért forgalom alapján határozza meg, hogy a böngésző hány párhuzamos TCP folyamot nyitott meg a **`www.bme.hu`** szerverhez!

Indokolja a válaszát! Használja a megjelenítés/analízis szűrőt és a **`netstat`** outputját is a feladat megoldásához!

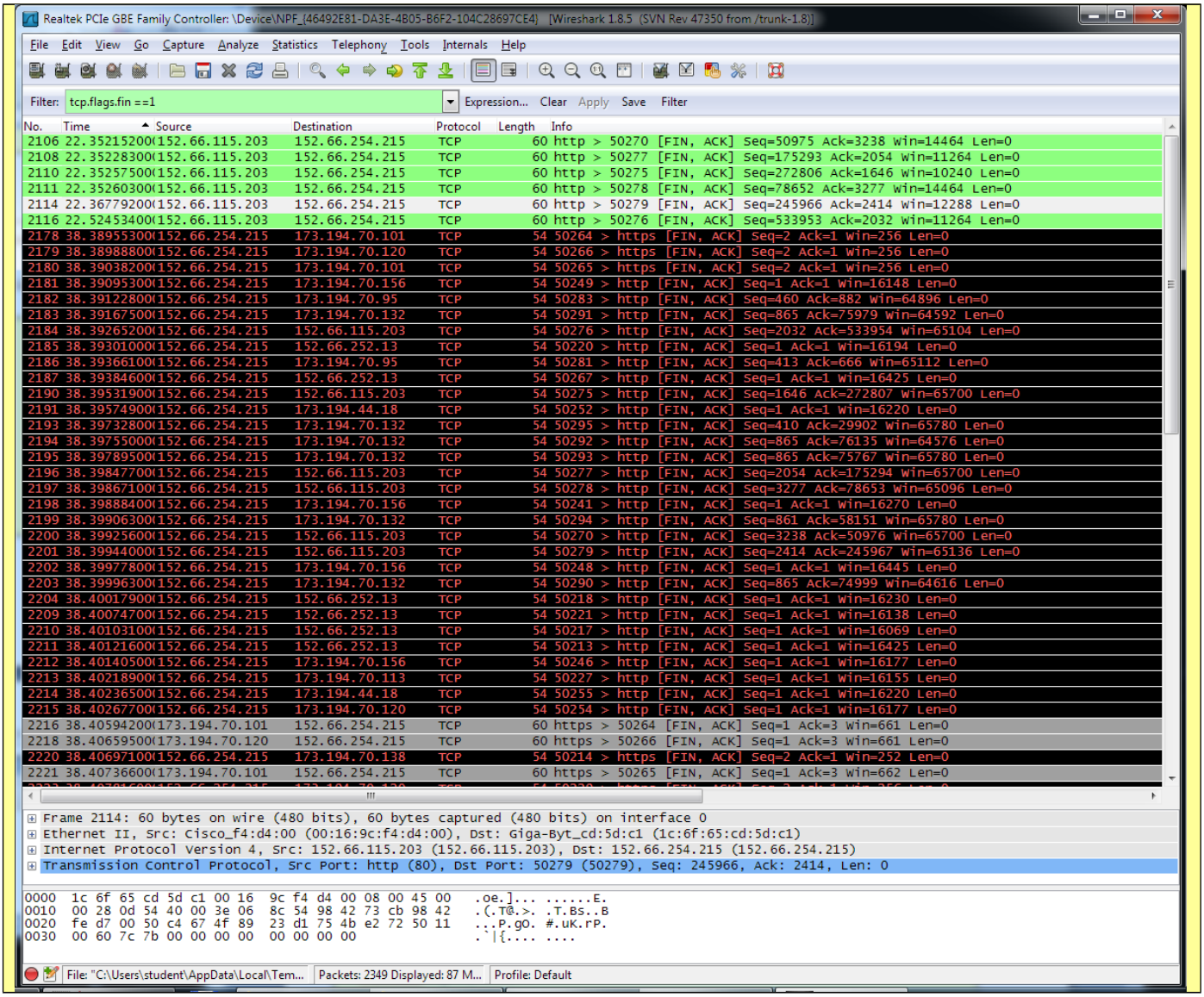
36 darab



5.6. Kapcsolatbontás

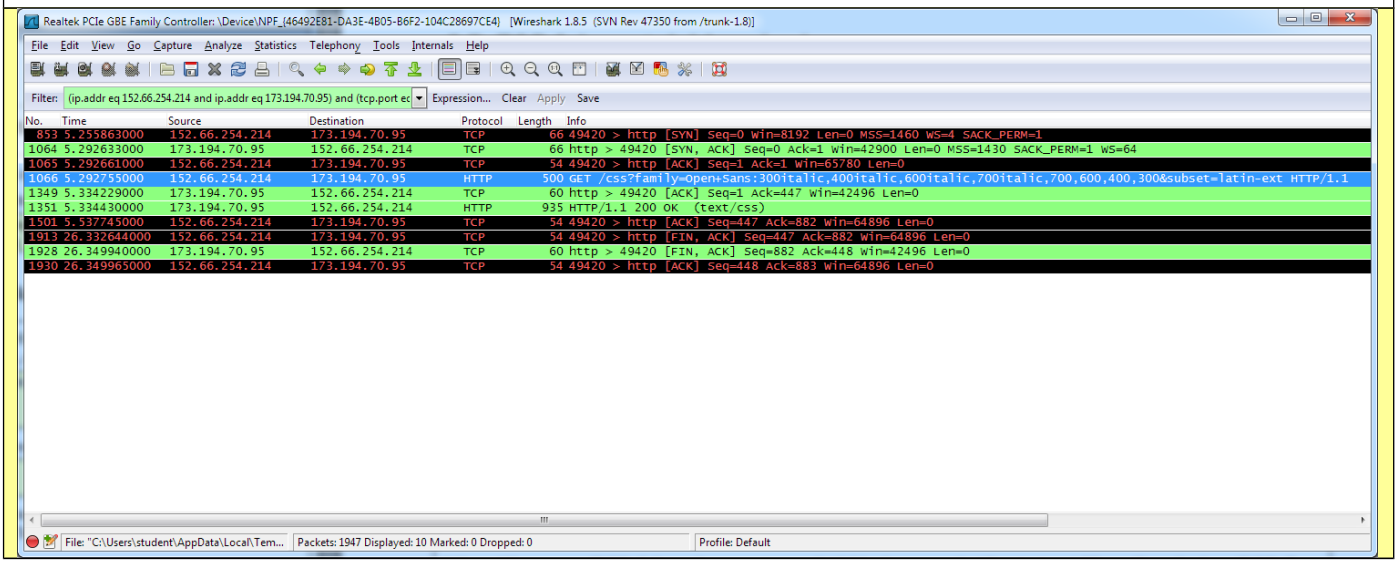
Hogyan és mikor történik a kapcsolat lebontása?

Készítsen a lebontás megtalálásához megjelenítés/analízis szűrőt, és használja a netstat outputot is!



5.7. TCP folyam tulajdonságai

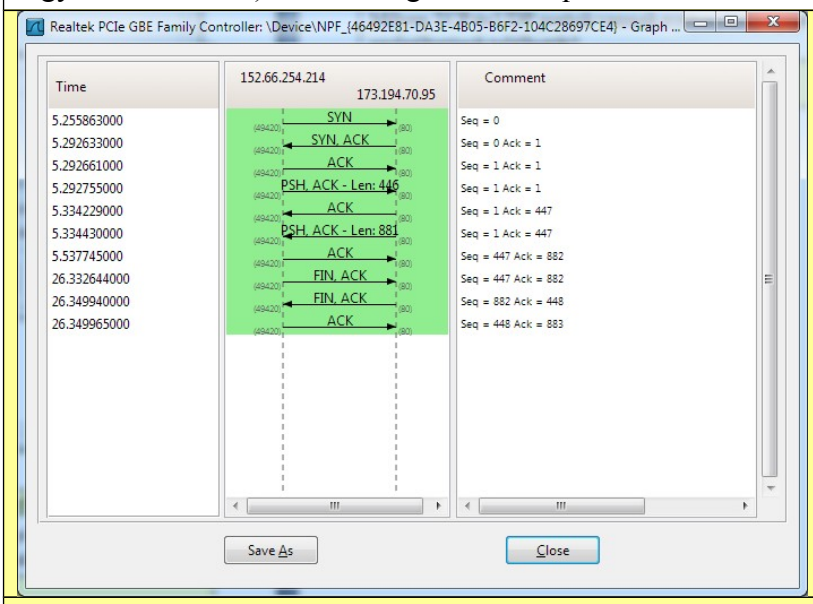
Szűrjük ki az egyik rövidebb (~10-15 üzenetből álló) TCP folyamhoz tartozó csomagokat (jobb gomb az egyik csomagon, majd *Conversation Filter / TCP*).



Sorrendben érkeztek a csomagok? Hogyan tudja ezt megállapítani?

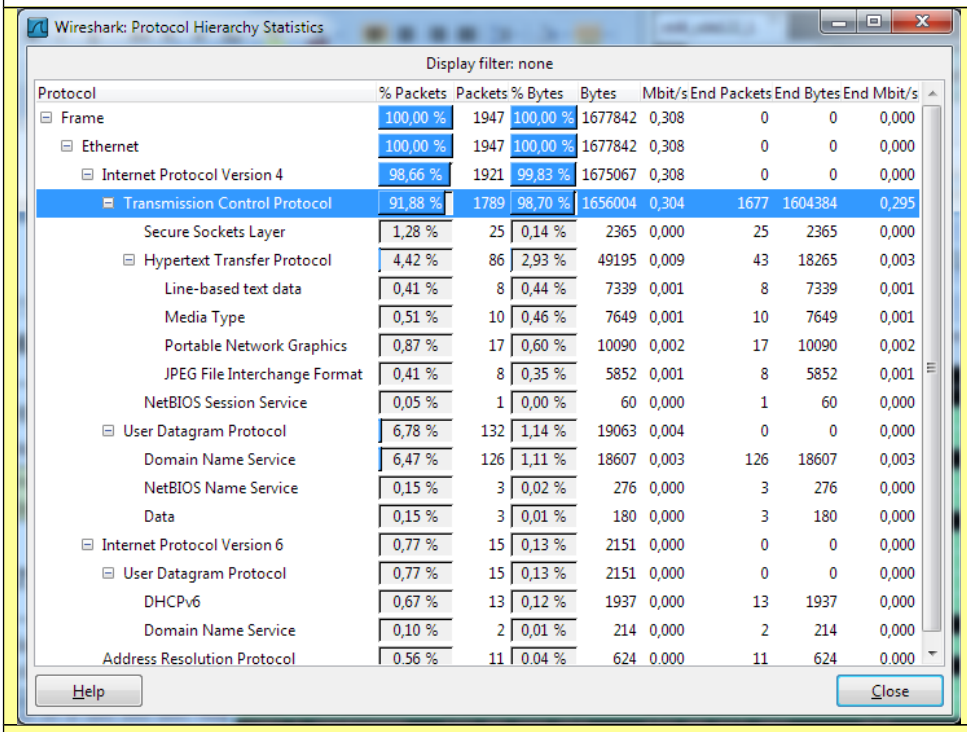
Sorrendben jöttek. A No. És Time oszlop tanulmányozásával lehet megmondani.

Vizsgálja meg a TCP folyamban az üzenetkülcdések menetét (*Statistics / Flow Graph*, és a *TCP flow* legyen kiválasztva)! Mire szolgálnak a Sequence number és Acknowledgment number mezők?



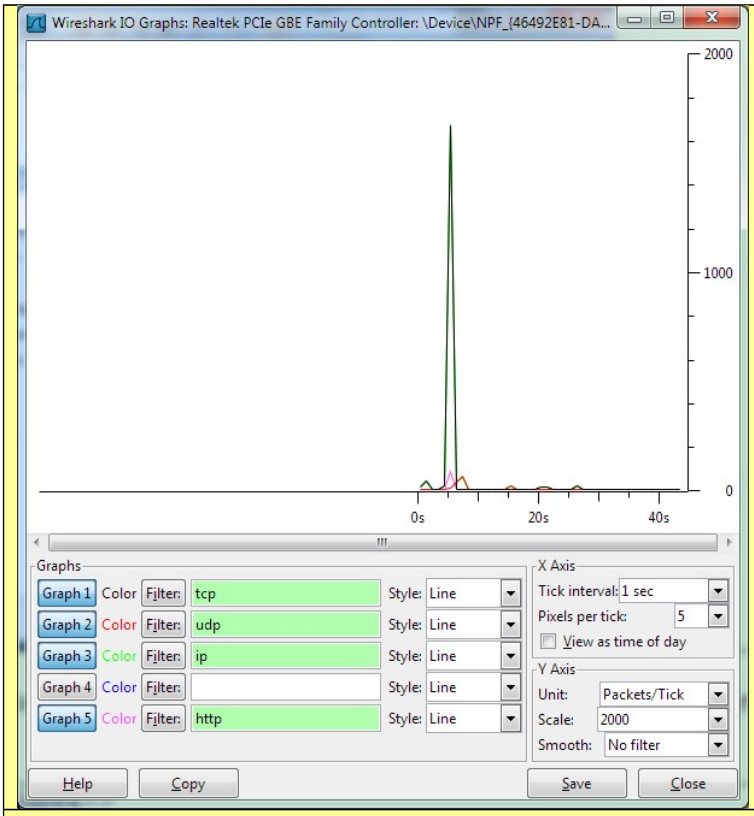
5.8. Protokollok sávszélesség-igénye

Ábrázolja a különböző protokollok által használt sávszélességet (byte/s) és csomaggyakoriságot (packet/s)! Indokolja a látottakat!



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	1947	100,00 %	1677842	0,308	0	0	0,000
Ethernet	100,00 %	1947	100,00 %	1677842	0,308	0	0	0,000
Internet Protocol Version 4	98,66 %	1921	99,83 %	1675067	0,308	0	0	0,000
Transmission Control Protocol	91,88 %	1789	98,70 %	1656004	0,304	1677	1604384	0,295
Secure Sockets Layer	1,28 %	25	0,14 %	2365	0,000	25	2365	0,000
Hypertext Transfer Protocol	4,42 %	86	2,93 %	49195	0,009	43	18265	0,003
Line-based text data	0,41 %	8	0,44 %	7339	0,001	8	7339	0,001
Media Type	0,51 %	10	0,46 %	7649	0,001	10	7649	0,001
Portable Network Graphics	0,87 %	17	0,60 %	10090	0,002	17	10090	0,002
JPEG File Interchange Format	0,41 %	8	0,35 %	5852	0,001	8	5852	0,001
NetBIOS Session Service	0,05 %	1	0,00 %	60	0,000	1	60	0,000
User Datagram Protocol	6,78 %	132	1,14 %	19063	0,004	0	0	0,000
Domain Name Service	6,47 %	126	1,11 %	18607	0,003	126	18607	0,003
NetBIOS Name Service	0,15 %	3	0,02 %	276	0,000	3	276	0,000
Data	0,15 %	3	0,01 %	180	0,000	3	180	0,000
Internet Protocol Version 6	0,77 %	15	0,13 %	2151	0,000	0	0	0,000
User Datagram Protocol	0,77 %	15	0,13 %	2151	0,000	0	0	0,000
DHCPv6	0,67 %	13	0,12 %	1937	0,000	13	1937	0,000
Domain Name Service	0,10 %	2	0,01 %	214	0,000	2	214	0,000
Address Resolution Protocol	0,56 %	11	0,04 %	624	0,000	11	624	0,000

A forgalom lényegében a TCP-n zajlott.



A http kis forgalommal jár.

5.9. Helyi hálózati szolgáltatások azonosítása * (csak az ötösért)

Milyen TCP és UDP portok vannak nyitva a helyi gépen a **`netstat`** alapján, és azokon milyen szolgáltatások találhatók?