

## Mérési utasítás

## Az ifconfig és a ping parancsok

# Az ifconfig parancs

Az ifconfig parancs a Linux hálózati paramétereinek beállítására szolgál. Amennyiben csak önmagában adjuk ki a parancsot, látható, hogy csak az éppen aktív hálózati interfészeket sorolja fel, a legfontosabb paraméterekkel.

root@feh	er4#:ifconfig
eth0	Link encap:Ethernet HWaddr 00:50:56:ae:00:34
	inet addr:193.224.129.168 Bcast:193.224.129.175 Mask:255.255.255.240
	inet6 addr: 2001:738:2c01:8000:250:56ff:feae:34/64 Scope:Global
	inet6 addr: fe80::250:56ff:feae:34/64 Scope:Link
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:17571 errors:0 dropped:0 overruns:0 frame:0
	TX packets:3135 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:1863396 (1.7 MiB) TX bytes:1104162 (1.0 MiB)
eth1	Link encap:Ethernet HWaddr 00:50:56:ae:00:35
	inet addr:10.9.0.200 Bcast:10.9.0.255 Mask:255.255.255.0
	inet6 addr: fe80::250:56ff:feae:35/64 Scope:Link
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:13415 errors:0 dropped:0 overruns:0 frame:0
	TX packets:7904 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:1741065 (1.6 MiB) TX bytes:3278014 (3.1 MiB)
10	Link encap:Local Loopback
	inet addr:127.0.0.1 Mask:255.0.0.0
	inet6 addr: ::1/128 Scope:Host
	UP LOOPBACK RUNNING MTU:16436 Metric:1
	RX packets:40232 errors:0 dropped:0 overruns:0 frame:0
	TX packets:40232 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:0
	RX bytes:4792781 (4.5 MiB) TX bytes:4792781 (4.5 MiB)

Amennyiben argumentumként megadunk egy interfész nevet, úgy csak a megadott interfészt fogja kilistázni.

root@feher	4#:ifconfig eth0
eth0	Link encap:Ethernet HWaddr 00:50:56:ae:00:34
	inet addr:193.224.129.168 Bcast:193.224.129.175 Mask:255.255.255.240
	inet6 addr: 2001:738:2c01:8000:250:56ff:feae:34/64 Scope:Global
	<pre>inet6 addr: fe80::250:56ff:feae:34/64 Scope:Link</pre>
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:17571 errors:0 dropped:0 overruns:0 frame:0
	TX packets:3135 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:1863396 (1.7 MiB) TX bytes:1104162 (1.0 MiB)

Az ifconfig parancsot használhatjuk beállításra is az alábbi szintaktikával:

ifconfig <interfész neve> <ip cím> netmask <netmaszk> up

Figyeljük meg az up kapcsolót: amennyiben az interfész **down** – azaz lekapcsolt – állapotban volt, úgy ezzel a kapcsolóval tudjuk aktívvá tenni. A Linux képes kiszámolni a megadott információk alapján a broadcast cím értékét, így azt nem kell megadnunk.

#### 1. Feladat.

 Állítsa be a fekete gép ethO ás interfészének a következő címet: 192.168.100.<190+gépszám> netmaszk: 255.255.255.0

(ifconfig eth0 192.168.100.194 netmask 255.255.255.0 up)

2. Majd ellenőrizzük sikerült-e átállítani az IP címet! (ifconfig eth0)

### A ping parancs

A ping parancs tipikusan hálózati elérhetőség tesztelésére használhatjuk. Segítségével ICMP echo üzenetet (lásd tankönyv) küldhetünk a kapcsolóként megadott hosztnak. Figyelem, a ping parancs kiadásakor a csomagokat addig küldjük a megadott hosztnak, amíg meg nem állítjuk. Ezt a <CTRL>+<C> billentyűkombinációval tehetjük meg.

```
root@cloud:~# ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
64 bytes from 10.9.0.1: icmp_req=1 ttl=64 time=1.79 ms
64 bytes from 10.9.0.1: icmp_req=2 ttl=64 time=0.292 ms
^c
--- 10.9.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.292/1.042/1.793/0.751 ms
```

Lehetőségünk van megadni pontosan hányszor "pingeljük" meg az adott hosztot, erre a -c kapcsolót használjuk.

root@cloud:~# ping -c 1 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
64 bytes from 10.9.0.1: icmp\_req=1 ttl=64 time=0.354 ms
--- 10.9.0.1 ping statistics --1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.354/0.354/0.354/0.000 ms

### 2. Feladat.

1. Ping parancs segítségével küldjön pontosan **10** ICMP ehco request üzenetet a 192.168.100.1es IP címre.



## Mérési utasítás A WireShark használata: TCP kapcsolatok analizálása

A WireShark (korábbi nevén Ethereal) a legfejlettebb hálózati sniffer és analizátor program. 1998-óta fejlesztik, jelenleg a GPL 2 licensz alatt. Nem igen találni ilyen széleskörű szolgáltatásokkal és ismeretekkel rendelkező hálózati analizátor programot. Támogatott operációs rendszerek: Windows, Linux, OS X, Solaris, FreeBSD, NetBSD és még sok egyéb. Grafikus interaktív interfésszel rendelkezik. Az OSI ISO modell 2-7 rétegének minden implementációját tudja analizálni. A program által jelenleg ismert protokollok száma jelenleg több mint 81000!

A WireShark analizátor funkcióit több könyv, illetve elektronikus irodalom írja le több száz oldal terjedelemben, így gyakorlaton csak az alap funkciókkal ismerkedünk meg.



### 1. Feladat.

Amennyiben nincs telepítve a számítógépre, telepítse a WireShark-ot.

apt-get install WireShark



#### Nézze át a WireShark kezelőfelületét!

<u>F</u> ile <u>E</u> d	lit ⊻ie	ew <u>c</u>	<u>Go C</u> a	pture	<u>A</u> na	alyze	<u>s</u> ta	atistics	<u>H</u> el	р											
ei u	0			6		×	¢		Q			Ŵ	Ŧ				Ð	Q	Q	+ +	V
📔 <u>F</u> ilter	:										•	E	<u>x</u> pre	ssior	🏷	<u>T</u> örlé:	s 🖌	<u>A</u> lkaln	naz		

Az első gombbal hívhatja elő a WireShark által elérhető és használható hálózati interfészeket.

🖸 Wirest	ark: Capture Interfaces					_ <b>-</b> ×
Device	Description	IP	Packets	Packets/s		Stop
🛒 wifio					<mark>≧(</mark> <u>S</u> tart	<u>الله O</u> ptions
🛒 ath0		192.168.1.112			<mark>≧(</mark> <u>S</u> tart	<u>الله O</u> ptions
🛒 eth4	1	.92.168.100.215	1223153	1192	<mark>≧(</mark> <u>S</u> tart	<u>مار O</u> ptions
🛒 any	Pseudo-device that captures on all interfaces		1223153	1192	<b>≧</b> ( <u>S</u> tart	<u>مار O</u> ptions
🛒 lo		127.0.0.1			<b>≧</b> ( <u>S</u> tart	<u>ما O</u> ptions
	×	<u>B</u> ezárás				

Ezen az ábrán láthatóak a "sniffelhető" interfészek, IP címekkel, és az áthaladt csomagok számával. A második gombbal állíthatja be az analizálás tulajdonságait.

<u>File Edit View Go Capture Analyze Statistics H</u>elp

<b>₩ <mark> </mark>₩                                     </b>	■ ቅ 🍋 🚡 👱 🛛 🔲 📑 🛛 🔍 🔍 🔍 🖭 🖬 🕍 ■ 🚽 🛧 Expression 🗞 Törlés 🖌 Alkalmaz
Wireshark: Capture Options Capture Interface: eth4 IP address: 192.168.100.215, fe80::21 Unk-layer header type: Ethernet ‡ [Capture packets in promiscuous mo	Il:11ff:febb:d801
Capture File(s)  File: Use multiple files	Browse  Browse  Display Options  Update list of packets in real time  Display Control of the control of
Stop Capture  after  after after  a	Name Resolution  Enable MAC name resolution  Enable getwork name resolution  Enable gransport name resolution  Enable gransport name resolution
<b>₩</b> Súgó	🗶 Mégsem 🛛 🎯 Start



## [SZÁMÍTÓGÉP-HÁLÓZATOK]

Széchenyi István Egyetem Győr Távközlési Tanszék

Legfelül látható, hogy jelen esetben az eth0-ás interfészt használjuk. A "Capture packet in promiscuous mode" kapcsolót mindig hagyja bekapcsolva, így ún. monitor módba állítja a hálókártyát. Be lehet állítani, hogy a WireShark fájlba mentse el az elkapott csomagokat. Megadhatja az analizálás leállásának feltételeit is, csomagszám, elkapott csomagok mérete és időkorlát alapján.

A Display options menüben lehet a csomagelkapás közbeni információkat beállítani. Automatikus "real-time" kijelzés, valamint ennek függvényében a képernyő görgetése, és az elkapott csomagok számának kijelzése.

Az utolsó részben va a névfeloldás lehetőségeinek beállítása, vagyis nem IP címeket kell ez esetben keresnie, hanem az ezekhez hozzárendelt szimbolikus neveket, valamint a MAC-ben az első 3 byte helyett a gyártó nevét.

A következő két gomb a csomag elkapás indítása, illetve leállítása.

### 2. Feladat.

Indítson egy csomagelkapást az eth0-án, úgy hogy a leállítás feltétele legyen 1 perc, valamint a képernyő automatikusan gördüljön a csomagokkal. (Nem kell menteni az előző listát, amennyiben a WireShark megkérdezné.) Ezután a böngészőt elindítva kérje le az *index.hu* honlapot.

PF         EX         Verse         O         Culture         Protocol         No           10.         Three         Secure         Protocol         No	- # # K						led) - wirestan	E) Dinti
Status         Status<				Help	alvze Statistics H	Capiture Analy	t Vew Go C	He. Ed
Effect         Image: Survey         Description         Table         Advance           10.         The         Source         Description         Processor         Source         Description           2 1, 252377         102, 108, 100, 215         102, 108, 100, 215         102, 108, 100, 215         102, 108, 100, 215         102, 108, 100, 215         102, 108, 100, 215         102, 108, 100, 216				a a a a x	* # #	e D	an or an	We Bal
MC (Ref)         Image: Control (1)         Image: Control (1)         Image: Control (1)         Image: Control (1)           10.         Time         Source         Destination         Protocol         Into         Source         Destination         Protocol         Into         Source         Destination         Protocol         Into         Source         Destination         Protocol         Into         Source			have be			- 10		-
No.         Time         Source         Destination         Photocal         Intel           2 7,528377         120,108,100,215         132,108,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         131,100,125         132,101,100,125 <t< th=""><th>100</th><th>tier A (trauns)</th><th>a. P1</th><th>* + Expres</th><th></th><th></th><th>1</th><th>Elber</th></t<>	100	tier A (trauns)	a. P1	* + Expres			1	Elber
27.570377       133.101.102.218       133.101.100.215       104.         27.574892       132.149.100.315       132.149.100.215       046.         27.574892       132.149.100.315       132.149.100.215       046.         27.574892       132.149.100.315       132.149.100.215       046.         27.575136       130.146.100.211       132.149.100.215       109.150.215         27.575136       132.149.100.215       132.149.100.215       129.450.100.215         27.575136       132.149.100.215       127.20.130.97       109.57711       540.159714       540.1497532 (120.160.255.159875757         37.56654       132.149.100.215       217.20.130.97       109.57711       54711       540.159714       5374154       540.1497532 (120.160.255.51598757555.515891557575         37.56654       132.158.100.215       217.20.130.97       109.255       57711       540.158.108.108.108.108.159.159.109.215       107.11 + way 140.11 540.140.14014581 Land 134-61565505.5156150.002.15       107.11 + way 140.11 540.2567 ###.449881 Land 134-6157657       124.148.148.148.149.149.149.149.149.149.149.149.149.149	-	da la	Protocol	Destination	De	Source.	Time	HO.
3 7,05%12       195,198,100.11       192,195,100.11       195       Standard quary AAAL LObe: Nutliburg. IN Section 2016         5 7,55%400       100,106,100.11       101,105,100.11       102,105,100.215       105       Standard quary AAAL LObe: Nutliburg. IN Section 2015         5 7,55%400       102,106,100.215       100,97       152,106,215       106       Standard quary AAAL LObe: Nutliburg. IN Section 2015       107         7 7,560520       217,20,106,107       152,198,100,215       107       www.sciffed       101,106,100,215       117,20,106,07       102,198,100,215       107       Standard quary AAAL LObe: Nutliburg. Unclide the Totel Photosystem Compared to the Comp		Landard query ARRA index.hu	DVG 7	32,168,100,1	00.225 18	152, 104, 100	2 7,874377	
<ul> <li>4.7,554882 192,169,100,215 192,105,100 106</li> <li>57,554802 192,106,100,215 217,20,130,57</li> <li>57,553138 192,166,100,215 217,20,130,57</li> <li>57,553138 192,166,100,215 217,20,130,57</li> <li>57,55521 217,20,130,57</li> <li>57,55624 192,106,100,215 217,20,130,37</li> <li>107,556420 217,20,130,57</li> <li>107,556420 217,20,130,57</li> <li>102,166,100,215 217,20,130,37</li> <li>107,556420 112,106,100,215 217,20,130,37</li> <li>107,556420 112,106,100,215 217,20,130,37</li> <li>107,556420 112,106,100,215 217,20,130,37</li> <li>102,166,100,215 217,20,130,47</li> <li>102,166,100,215 217,20,130,47</li> <li>102,166,100,215 217,20,130,47</li> <li>102,166,100,215 217,20,130,47</li> <li>102,166,100,215 217,20,130,47</li> <li>102,166,100,215 217,20,130,47</li> <li>107,156420 217,20,130,47</li> <li>108,160,218 107</li> <li>107,156420 217,20,130,47</li> <li>108,160,218 107</li> <li>107,156420 217,20,130,47</li> <li>108,160,218 107</li> <li>107,16742 217,20,130,47</li> <li>107,16742 217,20,130,47</li> <li>108,160,218</li> <li>109,160,110,110,128</li> <li>109,160,102,15</li> <li>109,160,102,15</li> <li>109,160,102,15</li> <li>109,160,102,15</li> <li>109,160,102,15</li> <li>100,114,1106,480,01</li> <li>100,114,1106,480,01</li> <li>100,114,1106,480,01</li> <li>101,1106,480,01</li> <li>101,1</li></ul>		tandard duery response	ING P	92.168.109.215	08.1 19	192.168.108	3 7:57/612	
5 7,594000         100,100,100,21         101,105,100,27         102         Standard augree (equiling (equiling), equiling)           6 7,550120         102,106,100,215         217,20,120,97         102         5711 > ww (5M) Sequel Augree (Augree (Aug		tandard query AAAA index.hu.tilb.sze.hu	UNS F	92,168,100.1	00.215 195	192.168,100	4 7,574650	
6 7.553136       100,100,100,211       217,20,130,97       100       57711 5 %       58711 5 %<		fandard query response, Ne such name	ING 3	02 168 105 215	00.1 100	192,168,100	5 7.574902	
7.7.580500       217.20.130.097       152.188.100.215       217.20.130.07       TOP       SVM = X STUL = WW 14X1 Seque Adva ty Mindbed Lemon Besteled TSM-557802         8.7.550825       100.108.100.215       217.20.130.07       TOP       STUL = WW 14X1 Seque Adva ty Mindbed Lemon Besteled TSM-557802         10.7.550825       100.108.00.215       217.20.130.07       TTP       CT / HTP / L1       Seque Adva ty Mindbed Lemon Besteled TSM-557802         11.7.650826       217.20.130.07       100.108.100.215       TOP       Seque Adva ty Mindbed Lemon Besteled TSM-557802         12.7.650826       217.20.130.07       100.108.100.215       217.20.130.97       TOP       STUL = WW 14X1 Seque Adva ty Mindbed Lemon TSM-5786 Lemon TSM-65786         13.7.654766       100.108.100.215       217.20.130.07       TOP       STVI = WW 14X1 Seque Adva ty Mindbed Lemon TSM-67962 Standov         15.7.65496       100.108.100.215       217.20.130.07       TOP       STVI = WW 14X1 Seque Adva ty Mindbed Lemon TSM-67962 Standov         15.7.65496       100.108.100.215       217.20.130.07       TOP       STVI = WW 14X1 Seque Adva ty Mindbed Lemon TSM-67962 Standov         16.7.56408       100.108.00.215       107.308.100.215       TOP       STVI = WW 14X1 Seque Adva ty Mindbed Lemon TSM-67067512 TSM-579716         16.7.66409       101.108.100.101       Fore seque Adva ty Mindbed Lemon TSM-67067512 TSM-57716	and a set	7711 > swx [StN] Seg=0 Lan=0 P65+1460 T92+87007505 T939+0 x5+4	102 3	17.20.130.97	00,219 213	192,168,300	6 7.575139	
87.585549       192.185.100.215       217.20.130.07       HTTP       Str1 / HTTP:1.1       10         107.586405       217.20.130.07       192.169.100.215       217.20.130.07       HTTP Str21 / HTTP:1.1       11         107.586405       217.20.130.07       192.169.100.215       107.0150.07       192.169.100.215       107.111.01         127.506405       217.20.130.25       217.20.130.07       192.169.100.215       107.111.01       4 recorded the fold         127.506405       110.2181.100.215       217.20.130.07       102.169.100.215       107.111.01       4 recorded the fold         137.504405       110.2181.100.215       217.20.130.07       102.169.100.215       107.111.01       4 recorded the fold         137.504405       117.501.304.110.215       217.20.130.07       102.169.100.215       107.111.01       4 recorded the fold         137.504405       117.501.304.110       217.20.130.07       102.105.100.215       102.111.01       1 recorded the fold         137.504405       117.501.08.101.215       217.20.130.07       101.12       1 recorded the fold       1 recorded the fold         137.504405       117.501.08.100.215       117.501.08.100.215       107.111.010.010.01       1 recorded the fold       1 recorded the fold         147.504405       117.501.08.100.01.01	SOE THERE	W > 57711 1978, ACKI Segro ACK=1 W1015792 Len=0 M95/1450 TSV=57597356 THER	1(P )	92.198.100.215	0.97 193	217.20.130.	7.7.580520	
0 7.566450       120.100.100.215       121.00.100.07       102.068.00.215       TCP       www = 57711 [4X] Seq=50 works with=Size [2016]         11 7.556458       217.20.150.57       102.068.00.215       TCP       TCP stopent of a reasonable with=Size [2016]         12 7.556458       217.20.150.07       102.168.00.215       TCP       TCP stopent of a reasonable with=Size [2016]         13 7.654765       127.30.130.07       102.168.00.215       TCP       TCP stopent of a reasonable with=Size [2016]         14 7.556458       217.20.130.07       102.168.00.215       TCP       TCP stopent of a reasonable with=Size [2016]         14 7.556458       217.20.130.07       102.168.00.215       TCP       TCP stopent of a reasonable with=Size [2017]         14 7.556459       127.20.130.07       102.168.00.215       TCP       TCP stopent of a reasonable with=Size [2017]         14 7.556459       127.20.130.07       102.168.00.215       TCP       TCP stopent of a reasonable with=Size [2017]         15 7.656459       127.20.130.07       102.168.02.100.215       TCP       TCP stopent of a reasonable with Size [2017]         14 7.55746       127.20.130.07       102.168.100.215       TCP       TCP stopent of a reasonable of C01         15 7.65459       127.20.130.07       001.161.010.050.01       TCP stopent of a reasonable of C01	156	77L1 # WWW [ADX] 54041 ADX41 W1043840 Leni+0 75848709/506 758946758/558	100	17.20,190.97	00.215 21	192, 168, 100	8 7.580549	
10 7,500-50     217.20,100.00     100.100,100     100.100     100.00     100.0000     100.000     100.000 <td< td=""><td></td><td>T / H10/1.1</td><td>HEIP 6</td><td>17.20.130.97</td><td>00.215 211</td><td>197.168.100</td><td>9 7.568625</td><td></td></td<>		T / H10/1.1	HEIP 6	17.20.130.97	00.215 211	197.168.100	9 7.568625	
11 7.000000       217.20.100.00       102.100.00       100       107       100       107	17500	We > 01/11 [work] redsh working whisters have the pressure interation/pre-	TOP 3	92-166.100.215	1.97 19.	217.20.120.1	0 7,000409	
10.1.000102       10.1.00.101       10.1.00.101       10.1.000100       10.1.1.1.1.1.1.1.1.000         11.1.000102       10.1.000101       10.1.1.1.1.1.1.1.1.000       10.1.1.1.1.1.1.1.1.000       10.1.1.1.1.1.1.1.000       10.1.1.1.1.1.1.1.000         11.1.000102       10.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	A REPORT OF	THE SEGRET OF A CONSERVED POINT FOR A PROPERTY AND A THE AVAILABLE AVAI	TOP 1	82.168.100; 219 13.20.168.50	0.97 125	217,20,190,1	1.7,504638 9.9.254604	1
14 7.000709       10.100.000.015       217.20.130.07       TOP	propropa -	The second of a constant at their	ton i	A PARTY A DOLLAR	0.212 211	102.100.100	A ADDRESS	
10 3.664806       217.20.130.07       102.168.00.215       TCP       TCP secret of a respective control of a respective contrespective control of a respective contrespective contr	100000	TTEL & see [ STV ] Conclude and a 2007 street (ST)   seed TELSTICK.13 TELSTICK.13	1/22 - 1	12 30 330 37	01.205. 21	107 100 100	a 7 604700	1
Prame 540 (06 bytes an wire, 66 bytes captured) Prame 540 (06 bytes cap	100 000 000	TO sevent of a reassabled Onit	TOP 1	92 109 100 215	0.07 10	017 20 130	S 7 Adverte	
2000 00 11 11 bb d8 01 00 14 4f 20 40 55 08 00 45 00								
Rie - YongvetherXXXXB88A9U* 152 KB 00:00:25 [P: 548 D: 548 M: 0 Crops: 0	•	₫P: 548 D: 548 H, © Crops: 0	i.,£. .4 (5]	00 45 00	47 20 48 55 08 00 28 49 59 14 62 61 41 74 82 80 9 75 08 04 29 68 53 97 88 00 00 25	01 00 14 47 00 36 06 2a 74 73 81 03 00 01 01 08 184907 152 88	0 11 11 lab d8 0 0 34 95 23 40 0 1 d7 00 58 e1 7 0 36 e1 66 90 0 0/etherxXXXX38	0000 00 0010 00 0020 54 0038 00 File: "/tm
🐻 🚖 🔜 🔲 2 = Mic - Foreitati Parent - 🛔 Male - Konguetor 👘	3 2:6	03 8	nqueror	II Pararita d Index - I	Mine -Texatabi-	R 2	EN.	13 6

## [SZÁMÍTÓGÉP-HÁLÓZATOK]



-Széchenyi István Egyetem Győr Távközlési Tanszék IV. Mérés

A WireShark az elkapott csomagok sorszámát, a forrás és cél IP-t, a protokoll nevét, valamint a csomag részletét jeleníti meg első látásra. Alul látható, hogy a WireShark a különböző protokollokat sorrendbe helyezi. Először a csomag méretét adja meg, majd az Ethernet opciókat. Itt található a forrás és cél MAC cím. Lejjebb az IP protokoll adatai láthatók, mint forrás és cél IP. Majd végezetül a TCP tulajdonságokat nézhetjük meg. (Mint például a forrás és cél port, valamint a különböző TCP bitek értékét (SYN, ACK, FIN, stb.).)

Jól megfigyelhető a képen, hogy először a mi gépünk lekéri a DNS bejegyzést a névkiszolgálótól, majd megkezdi IP cím alapján az index.hu kezdőlapját letölteni.

A hálózatokon sokszor rengeteg "szemét" csomag kering, mint például feszítőfa, illetve más egyéb routing protokoll. Ha ezeket figyelmen kívül szeretnénk hagyni, a csomagszűrőkhöz kell nyúlnunk.

Csomagszűrők két helyen alkalmazhatók:

- 1. csomagelkapásnál
- 2. megjelenítésnél

Ha csomagelkapásnál használunk szűrőt, akkor csak a szűrési feltételeknek megfelelő csomagokat fogja a WireShark eltárolni. Az eltárolt csomagok közül megjelenítési szűrővel választhatjuk ki, hogy melyek jelenjenek meg a képernyőn. (A két szűrő szintaxisa különböző!)

A csomagelkapási beállításokon (2. gomb) belül lehet csomagszűrőket alkalmazni.

A csomagszűrési beállításokon belül több előre definiált szűrő áll rendelkezésünkre.

SEtar:		•   + Darman	m by con	(Piller		
Tree     Tree	Casture Parks Casture Text Casture Text C	Constitution     Site 2, 999, 599, 599, 599, 599, 599, 599, 5	Net of the second secon	Charriert address 00.0 etternet type Gateloo Iso Disautant and no la Iso Disautant and no la Iso Address (14) (446.0.1 I Physical Address (14) (446.0.1) I	0.15.00.00.15 Weri Saturt	2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
00 00 14 47 30 40 55 10 10 34 15 64 40 50	00 11 11 10 08 01 40 08 42 12 (1) 48 10 55 36 25 00 00	00 00 43 00 .0 10 64 37 69 14	#			
b) (4) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	and the lot and out one	Unit day 1981 mill				

Meg lehet adni protokollszűrést, IP cím-szűrést, forrás és célport szűrést.



### 3. Feladat.

Hajtsa végre az előző feladatot, úgy hogy most filterként beállítva, csak a 80-as portot érintő kommunikációt vizsgálja. (*Capture Filter port 80*).

(Q)+411	ed - Worth	Terrine Andres Che	Index I hade		2 篇
-		BUX®	3 9 4 4 9 3	5 4 D	
जिमा जिमा			* 45	aession .	b Titles a second
Date: L	Time	Saista	Deutenting	Perture	e inter a constant de la constant de
1	0.00000	100.068.100.115	257.20.135.97	N/F	25436 S loop 16/ME langett Lawett Michigan Trans/2548386, Toppels Mich
2	0,009138-	217,20,130.97	362,169,300,215	5.21	www + 30408 1998, #043 Seg-0 Ack+1 Wine5782 Lone0 100+1400 T0#-57608712 T281+
-	0.005190	392, 168, 300, 215	217.20.120.97	RCP.	25436 > wax (ADA) Genyia Ackel waxesia40 Laneo Toyeetta40306 ToperStWoot12
	0,006067	192,388.300.215	257.20.130.97	HETP	OPT / HTTP/1.1
5	0.000064	227, 20, 130, 97	282,140,300,215	201	www.is.25406.(ADI). Select. Accessed warrended a served marketige and the second secon
	0.018124	217.20.190.97	282, 168, 100, 215	204	ITCP segment of a reasonabled PDUC
	5.016243	162, 168, 100, 215	267,20,130,97	504	THERE IS NOT [A(A) SERVICE SERVICES ADVICED Large TERMINES TERPS/S000715
	0.019289	207,20,180,97	292, 108, 109, 215	200	110 <sup>4</sup> segment of a revisement PDU
	C. CLOUDER	2007 00 100 00 -	2017-001-0000-001 2007-000-000-000	100	The content of a concentrate and the concentration
	O. OLIMANE	102.000.100.215	257, 20, 120, 97	100	Well a see 14/91 Second ashedde adveldes advelded Larvo TSARDTARMS TERSOTRATION
10	0.026410	217, 20, 136, 97	197, 169, 100, 215	104	TTCP sequent of a reasonabled PDC
13	0.020443	362,160,300,215	217.20.130.97	707	29406 F www TADAD Segr-441 Ackr/5/200 Min/17424 Lani-D 75/4/07/348281 T029-57508716
100	0.026546	217.90.190.97	292.168.100,215	3.04	TCP segrent of a realizatiled POLE
00 00 60 00 90 0f	14 4f 20 4 34 15 30 4 36 5c 74 5	9 25 00 15 11 Mt d8 0 00 40 06 a0 ms c0 0 50 16 73 cf 42 27 0 00 00 06 06 06 06 06	211 05 000 45 000 314 40 64 47 50 304.100.3 17 74 49 00 144.100.3 14 49 75 65 776	8.90 .81.6	
	THE PARTY OF THE	PART PLACE PLACE VE OF AL	at the ME can (W. 1404-444		10 2330 D 2330 H 2 Denne 2
an yere	Dec edizion	WWW. THEO UP UT OF	194		The state of state as a couple of
	1.44	A A A A A A A A A A A A A A A A A A A	Tearing Poreface   For	er rondoa	

Most csak a 80-as portot érintő kommunikációt jelenítjük meg.

#### 4. Feladat.

Hajtsa végre az előző feladatot úgy, hogy a csomagelkapás leállításának feltétele 3 csomag elkapása legyen. Ezzel az előző feladatból csak a "three-way-handshake", vagyis a 3 utas kézfogást kapjuk meg.

Ez a TCP protokoll kapcsolat-felépítési fázisa.



IV. Mérés



Ele Edit View Go Cepture Anelyze Statistics Help \$\$\$\$\$\$\$\$\$\$\$ b 🖬 × 0 🖧 Q + + • 7 2 📰 🖬 Q Q Q 🖂 \$\$\$ \$\$\$\$\$\$\$ Triber. Source or into 21.2.001.00 217.20 Prame 1 [74 Bytes on with, 74 Bytes Coptures) Effermet II, Srci Intel (b)de:01 100:1111:bb/d8/031, Osti Sundgrou,20:49/05 100:14147.20:445-520 Internet Portacol, Srci 102:106.000.215 109:158.000.2155, Dst. 217.20.100.97 (217.20.100.97) Transmission Control Aretocal, Src Part: 2007.135071, 2017 Purt: www.(300, 364; 0, Lam: 0 Provide a second state of the second Window size: 5040 Checksum: Oxed9b [correct] Options: 120 bytes) wmercococij, 38LP 296 Ruter 00.00.00 P 3D 3M 8 Drope of # m: - febete5 -- - Patar i ma 12:41 15 📤 😣 4 Cuntitled) - Wiresha

A csomagokat "kibontva" látható, hogy a 3 utas kézfogás egy TCP SYN-nel kezdődik, sequence number=0-val, majd a szerver visszaküldi a TCP SYN,ACK-t, egy sequence number=0 és Acknowledge number=1-el, amelyre a válasz egy TCP ACK, ahol mind a sequence number mind az acknowledge number 1-re van állítva.

Természetesen ezek csak jelen helyzetben ilyen értékűek a könnyebb megértés érdekében.

Ezzel létrejött a TCP kapcsolat.



### 5. Feladat.

Hajtsa végre az előző feladatot úgy, hogy vegye ki a csomagelkapás leállítási feltételt, és most – az egyszerűség kedvéért – a http://dev.tilb.sze.hu lapot kérje le!

Antina - Hory	Set 1	002000		= (#)
	al Po C × Pa	3 9 4 4 4 1	5 4 1	
Server and		+ +0	ressinn.	Special of glutman
to Thrue	times.	Inectination	Paint	el vo
1.0.000000	192 168 300 215	100.224-020.164	105	24300 S your FORM Generic Lando MOSCIARD TOwnship 2004
3 0.000212	199,229,129,264	192, 188, 100, 215	1129	way a "MURE CONV. AND Separt Active ViewS202 Lands With LOND TRAVENDERSTIN, TOPING
1 0.000232	192.168.300.215	168.304.139.164	TOP	34306 > www.CADK1_Gergh1_Ack+1_W1rt5840_Larr40_TSV+686000057_TSE8+154180776
4 0.000614	1907, 1888, 100, 215	188.224,129,184	HITP	CET / HTTV1.1
5 10 000991	199,229,329,164	182, 168, 100, 215	105	SWE & 34106 (AOC) Sept. ACCORD MINING LINCE TRANSMISSION TERMINACIES
6 0.001392	199.224.126.164	192, 368, 100, 215	HIM	HTTP/1.1 200 DC 11ex1/H10.5
7.0.001414	192,168-300.215	183.224.129.104	109.	SHIDE > www.LADK1_Seqr297_Advr394_W12v6962_Lerviti_TEX/000802857_T589v154188776
A IN START	1011.1204 120.154	100.108.100.215	112	we a petter child, can be and a second activities from the contraction of the second
9 15-049/01	192, 168, 100, 219	198.204.129.104	10*	34500 × MM TROYT 2604/20, MOV/240 AltivEntS Trueto LiterBSB/0618 12509/24084051
19 35.040301	192,168,190,215	193.229,129,109	100	SHOR > See [FIN, ACT] SEPTEM ACTION STANDS FOR TAMETORIES TRANSPORT
TE 36/04/2/5	193,224,127,104	132.300.000.215	100	ANA A BATRO CADAT DEBATRO ATMENDES FORMO CONCEASION OF ADMINISTRATION
				and a second s
Enguerce rude Acknowladgeme Hager length Window size: 0 Checksige: 0h7 9 Options: 112 5 9 (SED/ACK analys	ri 364 (relative o t materi 367 (rela 32 bytes 36, 600 36, 600 36 (correct) steal eis)	nganter namber) Hise ack number)		
000 00 11 11 00 0 000 00 34 34 48 020 04 07 00 50 1 000 00 36 78 43	29 01 00 14 81 20 46 10 00 37 06 15 77 01 27 38 46 34 23 77 55 00 00 31 01 08 06 09	15         00         00         45         00           etc         81         a4         02         35         . 4.149, F           57         37         16         90         12         . 4.149, F           30         ab         47         15         40         . 6	0 DJ. E.	B: 110 11 M Offeren 1
		Ban - Prat	INCOMPANY.	the same from
	3 4 20.00	titled) - wireshark		

Itt az utolsó négy csomagban megfigyelhető a 4 utas kézfogás, mely a TCP kapcsolat lebontását jelenti. Először a szerver küld egy FIN bitet, amelyre ACK a válasz, majd megy egy FIN, amelyre a szerver válaszol ACK-val.

