

Mérési utasítás

ifconfig, ping, WireShark használata

Az ifconfig parancs

Az ifconfig parancs a Linux Ethernet interfészek (hálózati vezérlők) hálózati paramétereinek beállítására, és az aktuális beállítások és állapotok kiíratására szolgál. Paraméterek nélkül használva, csak az éppen aktív hálózati interfészeket sorolja fel, a legfontosabb paraméterekkel.

Például:

```
root@feher4#:ifconfig
enp11s0 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)
enp11s0 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)
```

```
lo 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)
```

Ha a parancs argumentuma egy interfész, akkor csak a megadott interfészt beállításait jeleníti meg.

Például:

```
root@feher4#:ifconfig enp11s0
enp11s0 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)
```



Széchenyi István Egyetem Győr Távközlési Tanszék

Fontos még a -a paraméter is. Segítségével az összes interfész (beleértve a nem aktívakat is) beállításai kiírathatóak.

Az ifconfig parancs segítségével lehet beállítani is az egyes interfészeket a következő szintaxis alkalmazásával:

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

Amennyiben egy interfész **down** azaz lekapcsolt állapotban van, úgy az up kapcsolóval lehet azt aktívvá tenni. A Linux képes kiszámolni a megadott információk alapján a broadcast cím értékét így azt nem kell megadnunk. Fontos megjegyezni, hogy az ifconfig parancs segítségével elvégzett beállítások csak a legközelebbi újraindításig maradnak meg.

Feladatok

1. Indítsa el a terminál (konzole) programot, mely ekvivalens azzal a terminállal amiben eddig dolgozott.

K menü -> Alkalmazások -> Rendszer -> Terminál

- Írassa az összes interfészt, és állapotukat! Hány interfészt lát? ifconfig -a
- Állítsa be a fekete gép enp11s0 interfészének a következő IP címet 192.168.100.190+gépszám. Majd adja meg az alapértelmezett hálózati átjárót és a DNS kiszolgálót.

```
ifconfig eth1 down
ifconfig eth1 192.168.100.{190+gépszám} netmask 255.255.255.0 up
route add default gw 192.168.100.1
echo "nameserver 192.168.100.2" > /etc/resolv.conf
```

 Ellenőrizze, hogy sikerült-e beállítani az IP címet ifconfig ethl

A ping parancs

A ping parancs a hálózati kapcsolat tesztelésére szolgál. Segítségével ICMP echo üzenetet (lásd tankönyv) lehet küldeni a paraméterben megadott hosztnak. Linux esetében a ping parancs a csomagokat addig küldi a megadott hosztnak, míg leállításra nem kerül. Ezt a <CTRL>+<C> billentyűkombinációval lehet megtenni.

Például:

```
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
```

IV. Mérés



[SZÁMÍTÓGÉP-HÁLÓZATOK]

Lehetőség van megadni, hogy a parancs pontosan hány ICMP echo request üzenetet küldjön a célállomás felé. (Hányszor "pingeljük" meg az adott hosztot.) Ezt a -c kapcsoló segítségével lehet megtenni.

Például:

```
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
```

Feladatok

- 1. Kérdezze le a ping parancs paramétereit, majd tanulmányozza azokat! (ping)
- 2. A ping parancs segítségével küldjön pontosan 10 ICMP ehco request üzenetet a 192.168.100.1-es IP címre. Tanulmányozza az eredményeket! Milyen átlagos és maximális válaszidőket tapasztalt? (ping -c 10 192.168.100.1)

WireShark program alkalmazása

A WireShark (korábbi nevén Ethereal) egy rendkívül fejlett hálózati sniffer és analizátor program. Fejlesztése 1998-óta folyik, jelenleg 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 több mint 81000, de bárki készíthet hozzá újabbakat.

A WireShark analizator funkcióit több könyv, illetve elektronikus irodalom írja le több száz oldal terjedelemben, így a gyakorlat keretében csak az alap funkciókkal ismerkedünk meg.

Feladatok

- 1. Amennyiben nincs telepítve a számítógépre, telepítse a WireSharkot az apt install wireshark parancs kiadásával!
- 2. Indítsa el a programot, majd nézze át annak kezelőfelületét!

A wireshark indításnál automatikusan láthatóak a "sniffelhető" interfészek, IP címeikkel, használati grafikonnal.

_	The Wireshark Network Analyzer	~
File Edit View C	Go Capture Analyze Statistics Telephony Wireless Tools Help	
()	I I II	
Apply a display filter	r <ctrl-></ctrl->	Expression +
	Welcome to Wireshark Depture using the file iter a capture filer any Iteration any Iterating Bandaring	
Ready to load or o	capture No Packe	ets Profile: Default
👯 🏮 Villamosmér	rnöki szak, Távközlés-in 📔 root : bash — Konsole 🛛 🧖 The Wireshark Network Analyzer	🖻 🖳 🗣 🔺 12:58 ≡

A negyedik gombbal állíthatja be az analizálás tulajdonságait.

			~ ^ 🕲	Jev Villamosm		k, Távköz			SZE - Győr) - Mozilla Firefox 🗸 \land 🚫
File	Edit View Go Capture A	nalyze Statistics Telepho	ny Wireless Tools Help	J 🚯 Villamos	imérnöki si	zak, T	× (+		
			· K > 📮 📘 🕨	(¢) 🖗 h	ttps://www	v.tilb. sze	.hu	C Q Keres	iés ☆ 自 » =
	ply a display filter <ctrl-></ctrl->	Wiresha	Expression +	0 t ¥	5	összese	n:7 ? ∨ ^ ⊗	- + 1009	% + >> Name Resolution Passive MAC addresses Insekve metoack-layer names
	output Options							ibyte(s) =	Resolve transport layer name Whe external network name resolver
In	terface	Traffic	Link-layer Header	Promiscuous	Snaplen ((B Buff	er (MB	(8)() ¥	Set Decirio
>-	enp11s0	hand had had had	l⊶ Ethernet		default	2	-	-	
	any	hour har har har har har har har har har ha	Linux cooked		default	2	-	s0 interfészt h	nasználjuk. A "Capture packet in
>-	Loopback: lo		Ethernet		default	2	-	odba állítja a	hálózati kártyát, melyben olyan
>-	docker0		Ethernet		default	2	-		Készítette: Kovács Á
	nflog		Linux netfilter log messages		default	2			
	nfqueue		Raw IPv4		default	2			
	usbmon1		DLT -1		default	2	-		
	usbmon2		DLT -1		default	2	-~		
Cap	Enable promiscuous mode on all in	terfaces			•	Manage C	Interfaces ompile BPFs		IV. Mérés
8	Súgó SSH remote capture: ssh			csomagokat. I	Vegadhatja	Start a az ana	8 Bezárás alizálás leállásán	számítógépünkr t is, hogy a Wir ak feltételeit is,	nek szólnak. Ezt a kapcsolót mindig eShark fájlba mentse el az elkapott , csomagszám, elkapott csomagok
					A Display options merüben lehet a csomagelkapás közbeni információkat beállítani. Automatikus real-itme' ilyitzés, valamint ennek függvényében a képernyő görgetése, és az elkapott csomagok számának kijelzése is itt állítható be. Az utolsó részben lehet beállítani a névfeloldás működését, ekkor nem IP cimeket lehet látni, hanem az ezekhez hozárendét szímbolikus neveket, valamint a MAC címben az első 3 byte helyett a gyártó neve jelenik meg.				
Learn User's Guide · Wiki · Questions and Answers · Mailing Lists You are running Wireshark 2.2.6 (Git Rev United and State State).				A következő két gomb a csomag elkapás indítása, illetve leállítása. 3. ICMP vizsgálata Indítson egy csomagelkapást az enp11s0 interfészen! (Ha a program megkérdezné, úgy nincs szükség az előző adatok mentésére). Miközben a WireShark az adatokat gyűlti, adon ki egy ping -c 4 192.168.1090.1 parancsot Mikóta a ping parancs végzett, állítsa le a WireShark programban a csomacok elkapását! Elemezze ki az eredményeket!					
2	Ready to load or capture	No Packet	s Profile: Default	A Firefox an hogy javith	utomatikus iassuk a fel	san adat lhasználo	okat küld a Mozi ói élményt	lla számára,	Megosztandó adatok ki <u>v</u> álasztása 🛛 🗙
ŵ	🕑 Villamosmérnöki szak, Távközle	és-in 📄 root : bash — Kor	nsole 🔀 The Wir	eshark Network A	alyzer	Z	Wireshark · Capt	ure Interfaces	≣ 🖫 🗣 🔺 13:01 ≡



Széchenyi István Egyetem Győr Távközlési Tanszék

Legfelül látható, hogy jelen esetben az **eth1** interfészt használjuk. A "Capture packet in promiscuous mode" kapcsoló ún. monitor módba állítja a hálózati kártyát, melyben olyan csomagokat is el tudunk kapni, melyek nem a mi számítógépünknek szólnak. Ezt a kapcsolót mindig kapcsoljuk be a mérések során. Az options menüpont alatt be lehet állítani azt is, hogy a WireShark fájlba mentse el az elkapott csomagokat. Megadhatja az analizálás leállásának feltételeit is, csomagszám, elkapott csomagok mérete és időkorlát alapján.

The Weekhack Measure Markey Wieekhack Measure Markey Statistics Telephony Wieeks Tools Help Pie Edit View Go Cauve Analyze Statistics Telephony Wieeks Tools Help Wieeksan Kalkan Statistics Telephony Wieeks Tools Help Pie Edit View Go Cauve Analyze Statistics Telephony Wieeks Tools Help Wieeksan Kalkan Statistics Telephony Wieeks Tools Help Pieupity a displar (filer Wieeksan Kalkan Statistics Telephony Wieeks Tools Help Wieeksan Kalkan Statistics Telephony Wieeks Tools Help Piputo Output Options Name Resolution Piputo Output Name Resolution Namataitatanataitaita Name Network names		
File Edit. View Go Cupture Analyze Statistic Telephony Wireless Tools Help Villamonnémoki szak. T. * + 	The Wireshark Network Analyzer V 🔨 🚫	Villamosmérnöki szak. Távközlés-informatikairány honlapja (SZE - Győr) - Mozilla Firefox 🗸 \land 🔇
Image: State of packets Image: State of packets Image: Image: State of packets Image: State of packets Image: Im	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	/ 🖚 Villamosmérnöki szak, T 🗙 🕂
Apply a display filter = Citi-0 Imput Output Options Name Resolution Imput Imput Output Options Name Resolution Imput Imput Imput Output Options Name Resolution Imput Imput Imput Output Options Name Resolution Imput	▲ ■ ⊿ ⑧ □ □ 🛯 🖉 🖉 Q < > > K > I 🜉 📕 >	🔄 🛈 🔒 https://www.tilb.sze.hu 🛛 C 🔍 Keresés 🔄 😭 🕷 🚍
Wireshark Copure Interfaces Image: Copure Interfaces Image: Copure Interfaces Imput Output Options Name Resolution Imput Output Options Name Resolution Imput Output Resolve MAC Addresses Imput Impu <	Apply a display filter <ctrl-></ctrl-> Expression +	🔟 🛧 🖡 5 összesen: 7 — 🗕 🕂 100% 🔹 🚿
Papet Output Options Name Resolution Display Options Name Resolution Update list of packets in reaktime Resolve MAC Addresses Automaticatily scoled uning ble capture Impact of packets in reaktime Impact of packets Resolve MAC Addresses Stop capture automatically after Impackets Impack of packets Resolve transport names Impackets Impackets Impacke	Wireshark · Capture Interfaces	? ∨ ∧ ⊗ Name Resolution
Display Options Name Resolution I Update list of packets in reak-line I Resolve NACK Addresses I Advantatically scroll during live capture Resolve network names I Show extra capture information dialog Resolve network names I I I Res I I I I Res I I I Res I I I I Res	Input Output Options	Fielder networkliger netwo
Update list of packets in real-time I update list of packets in real-time I works acquue information dialog Resolve transport names Show extra capture information dialog Resolve transport names Stop capture automatically storid during live capture I works acquue information dialog Resolve transport names Stop capture automatically storid during live capture I works acquue information dialog Resolve transport names Stop capture automatically after I works acquue information dialog Stop capture automatically after I works acquue information dialog Stop capture automatically after I works acquue information dialog Stop capture automatically after I works acquue information dialog Stop capture automatically after I works acquue information dialog Stop capture automatically after I works acquue information dialog Stop capture automatically after I works acquue information dialog Store capture sch I works acquue information dialog I works acquue	Display Options Name Resolution	a(a) w Stee external measure
Automatically scolid uring live capture Automatically scolid uring live capture Beacobe transport names Show extra capture information dialog Resolve transport names Stop capture automatically after I i packets I i packets<	Update list of packets in real-time Resolve MAC Addresses	Dark Useries
Show extra capture information dialog Resolve transport names Stop capture automatically after 1	Automatically scroll during live capture Resolve network names	s0 interfészt használjuk. A "Capture packet in
Stop capture automatically after 1 packets 1 i i i i i i i i i i i i i i i i i i i	Show extra capture information dialog Resolve transport names	dba állítja a hálózati kártyát, melyben olyan
Stop capture automatically after 1 packets 1 files 1 <th></th> <th>Készítette: Kovács A</th>		Készítette: Kovács A
Image:	Stop capture automatically after	
Image: Suge V. Méré: Image: Suge Start Bezins Image: Start Bezins Start Image: Start Comago: Start Bezins Image: Start Comago: Start Bezins Image: Start Start Bezins Start Image: Start Bezins Start Bezins Image: Start Comago: Start Bezins Start Bezins Image: Start Start	□ 1	
Image: Sigged Start Example Italiagépünnek szőnak. Et a kapcolót mindig is, hogy a WireShark fájlás mentse al ar elkapott is, hogy a WireShark fájlás mentse al ar elkapott is, hogy a WireShark fájlás mentse al ar elkapott Image: Signed is sis signed is signed is signed is sis signed is sis sis signed is s	□ 1	
Image: Stage Start Examitiógépünknek szólnak. Ez a kapcsolót mindig b. k. nog a VireShark fájba mentse el az elkapott b. k. nog a VireShark fájba mentse el az elkapott SSH remote copture ssh Image: SSH remote copture ssh comagokat. Megidhatja az analizálás Tealfásinak feltetelet is, comagazám, elkapott comagok mérete és időkrinak melben lekt a comagelkapis közbeni informádókat beállitani. Automatikus "real-lime" kijzlése, valamit enek függvenyeben a képernyő görgetése, és az elkapott comagok számának kijzlése isi tállíthatő be. A Display option melben lekt a comagelkapis közbeni informádókat beállitani. Automatikus "real-lime" kijzlése, valamit a nek feldúlás működését, ékor nem IP címeket beálltáni, hanem az ezelben bozárnedek szimbölus neveekt, valamitt a MAC címben az első 3 byte helyett a gyáró neve jelenik meg. A következő két gomb a comagelkapis indtása, illerve leállitása. Im Scrissfala Indison egy comagelkapist az ep1150 interfészeni (Ha a program megkérdezné, úgy nics szükség az előő ádatok mense vágett, állítas le a WireShark programban a comasok elkapjáti I Elemezze ki az eredménveket! Y Ready to load or capture No Packets Profile: Default Profile: Default Megosztandó ádatok kigálaszámár. Megosztandó ádatok kigálaszámár.	□ 1 ↓ kilobytes ∨	IV. Mérés
Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Star (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Start (Interpretation of the start) Start (Interpretation of the start) Image: Star (Interpretation of the start) Start (Int	1 seconds Y	
Star		
Somapolat. Megađnitaja za nalizalas leališašnak faliba nentse el az elkapott somagokar. Somapolat. Megađnitaja za nalizalas leališašnak feltételeti (s. csomagskapis kobeni informátolkat beslittani. Automatuku renter kijetése) si kobeni informátolkat beslittani. Automatuku renter kijetése isi tá illitható be. A Display options meniben lehet a csomagekapis kobeni informátolkat beslittani. Automatuku renter kijetése isi tá illitható be. A utokó részben lehet basiltaria nevétetu salitaria a névfetoldsis működését, ekkor nem IP címeket lehet lámi, hanem az ereke hozzárendet szímbolikus nevéket, valamint a MAC címben az első 3 byłe helyett a gyártó neve jelenik meg. A következő két gomb a csomag elkapás indítása, illetve leállítása. Somagokat 22.6 (Git Rev Unknown from unknown). Vou are running Wireshark 22.6 (Git Rev Unknown from unknown). Ready to load or capture No Packets Profile: Default	🛱 Súgó	✓ Start 🛛 😵 Bezárás számítógépünknek szólnak. Ezt a kapcsolót mindig
 Shr ferinder öpplure skn Colmagozal, weightig az aninzulas reinstantas fereteteri is, Schnigzzah, eikapott Schlagozah, eikapott Sc		t is, hogy a WireShark fájlba mentse el az elkapott
A Display options merüben lehet a csomagelkapis közbeni információkat beállítani. Automatikus real-time" kijležes julia valamit emek fügevneben a kepernyő görgetése, és az elkapott csomagok számának kijelzés julia talak kijelzés julia valamit emek fügevneben a kepernyő görgetése, és az elkapott csomagok az utobó részben lehet beállítani a névfeöldős működését, ekkor nem IP cimelet lehet lálni, hanem az esekher hozzírendek és zinsöllsus nevéset, valamit a MAC cimben az első 3 byte helyett a gyrány neve jelenik meg. A következő két gomb a csomag elkapás indítása, illetve leállítása. J. (CMP vissgálata Indítson eneg csomagelkapási az enp11se interfészeni (Ha a program megkérdezné, úgy nincs szükség az első adatok mensekése). Műköben a VireShark az adatokat gyűt, adon ki egy prig - e somarok elkapásti Elemezze ki az erednénveketI	Son remote cupture son	mérete és időkorlát alapján.
************************************		A Display options menüben lehet a csomagelkapás közbeni információkat beállítani. Automatikus
Zalinalnik vjeztež v kladivali v portežev jednov stavali v v kladivali v v kladivali v v kladi v kladivali v kladivali v kladivali v kladivali v kladiv		"real-time" kijelzés, valamint ennek függvényében a képernyő görgetése, és az elkapott csomagok
Zu tobo Pszcemient cealinan a newetousa mukodasi tuskor nem r čimest cieret nam, name na ceskéh zbožárendet sámbolitus neveket, valamint a MAC cimben ar elo 3 byte helyett a gyárdo neve jelenik meg. Learn A következő két gyon a comag elkapás indítása, illetve leállítása. User's Guide - Wiki - Questions and Answers - Malling Listsj You are running Wireshark 22.6 (Git Rev Unknown from unknown). 3. ICMP vizsgálata Indítison eregi somag elkapás at enp1150 interfészeni (Ha a program megkérdezné, úgy nics szülség az előő ádatok mensens végzett, allitsa le a WireShark za atotkat gyűt, adjon ki egy ping - e 4. 1922. IEB. 100-1. parancsot tituktian a ping parancs végzett, allitsa le a WireShark programban a comanok elkapásitus an adotka kuld a Mozilla számára. W Ready to load or capture No Packets Profile: Default Megosztandó ádatok kuld a Mozilla számára. Megosztandó ádatok kuldá a kozilla számára.		Szamanak Njerzese is itt anitriato be.
Image: Standing of the standing standi standi standing standing standing standing standing standing sta		az ezekhez hozzárendelt szimbolikus neveket, valamint a MAC címben az első 3 byte helyett a gyártó
Zers Guide Witki · Questions and Answers · Mailing Listsj A következő két gomb a csomag elkapás indítása, illetve leállítása. Varer Guide · Wiki · Questions and Answers · Mailing Listsj S. (CMP vissgalta) Vou are running Wireshark 22.6 (Git Rev Unknown from unknown). A föreföx adrots mentsérée). Miközben a Wireshark za aktokat gyűjt, adjon ki egy ping - c Varer unning Wireshark 22.6 (Git Rev Unknown from unknown). S. (CMP vissgalta) Profile: Default Marching ping paramas végett, allitsa le a Wireshark programma a csomasok elkapásít Elemezze ki az eredménveket! Profile: Default Marching ping paramas végett, allitsa le a Wireshark programma a csomasok elkapásít Elemezze ki az eredménveket!		neve jelenik meg.
Learn 3. (CMP vissglata User's Guide * Wiki * Questions and Answers * Mailing Lits! a roor running Wireshark 22.6 (Git Rev Unknown from unknown). Vare's Guide * Wiki * Questions and Answers * Mailing Lits! a roor running Wireshark 22.6 (Git Rev Unknown from unknown). Vare's Guide * Wiki * Questions and Answers * Mailing Lits! a roor running Wireshark 22.6 (Git Rev Unknown from unknown). Vare's Guide * Guide		A következő két gomb a csomag elkapás indítása, illetve leállítása.
User's Guide Wiki Questions and Answers Mailing Lists You are running Wireshark 22.6 (Git Rev Unknown from unknown). 4 192.168.108-1, parancsot Murán a ping parancs végzett, alltsa le a WireShark programman. W Ready to load or capture No Packets Profile: Default The April Andorski a Cablack and Anzilla számára. Megosztandó adatok kiúla a Mozilla számára.	Learn	3. ICMP vizsgálata
You are running Wireshark 2.2.6 (Git Rev Unknown from unknown). 4 192.168.100-130 aparacost Miután a ping parancos végzett, álltsa le a WireShark programbana somack elkadoást Elemezze ki az eredménvekett Z Ready to load or capture No Packets Profile: Default Marcia számára. Megosztandó adatok kiúld a Mozilla számára.	User's Guide 🕐 Wiki 🕐 Questions and Answers 🕐 Mailing Lists	az előző adatok mentésére.) Miközben a WireShark az adatokat gyűjti, adjon ki egy ping -c
P Ready to load or capture No Packets Profile: Default Profile: Default Megosztandó adatok kiúli a Mozilla számára. Megosztandó adatok kiúli a Mozilla számára.	You are running Wireshark 2.2.6 (Git Rev Unknown from unknown).	4 192.168.100.1 parancsot! Miután a ping parancs végzett, állítsa le a WireShark programban a csomagok elkapását! Elemezze ki az eredményeket!
Ready to load or capture No Packets Profile: Default ^W hogy javíthassuk a felhasználói élményt. Megosztando adatok kyalasztasa *		A Firefox automatikusan adatokat küld a Mozilla számára,
	Ready to load or capture No Packets Profile: Default	hogy javíthassuk a felhasználói élményt. Megosztando adatok kigalasztasa

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 is itt állítható be.

Az utolsó részben lehet beállítani a névfeloldás működését, ekkor nem IP címeket lehet látni, hanem az ezekhez hozzárendelt szimbolikus neveket, valamint a MAC címben az első 3 byte helyett a gyártó neve jelenik meg.

A legelső 2 gomb pedig a csomagelkapás elindítása illetve leállítása.

3. ICMP vizsgálata

Indítson egy csomagelkapást az eth1 interfészen! (Ha a program megkérdezné, úgy nincs szükség az előző adatok mentésére.) Miközben a WireShark az adatokat gyűjti, adjon ki egy ping -c 4 index.hu parancsot! Miután a ping parancs végzett, állítsa le a WireShark programban a csomagok elkapását! Elemezze ki az eredményeket!

A WireShark az elkapott keretek sorszámát, a forrás és cél IP címet, a protokoll nevét valamint a csomag részletét jeleníti meg első látásra. A program felső ablakában keresse meg az első ICMP Echo request csomagot, és válassza ki azt! Ekkor a középső ablakban megjelenik a kiválasztott csomaghoz



Széchenyi István Egyetem Győr Távközlési Tanszék

tartozó keret, ahol részletesebben is elemezheti azt. Vegye észre, hogy az egyes hálózati rétegek jól megfigyelhetőek ebben a középső ablakban! A legelső sor a keret paramétereit tartalmazza, majd alatta az Ethernet keret, az arra épülő IP, legvégül pedig az ICMP.

No.	Ti	me	Source	Destination	Protocol	Length Info
	10	.0000000	0192.168.43.241	192.168.43.1	DNS	68 Standard query 0x468b A index.hu
	20	. 3671 520	0102 169 42.1	192.100.43.241	DNS	84 Standard quely - terence 0x468b A 217.20.130.99
		.3944610	0192.168.43.241	217.20.130.99	ICMP	74 Echo (ping) request id=0x0001, seq=/ 53/64283, ttl=128 (reply
	41	.8583970	217.20.130.00	102 168 13 241	TCMP	74 Echo (ping) repl) 1d=0x0001, seq=7163/64283, ttl=55 (reques
	51	.8753230	0192.168.43.241	217.20.130.99	ICMP	74 Echo (ping) request id=0x0001, seq=7164/64539, ttl=128 (reply
	62	.1669810	0 217.20.130.99	192.168.43.241	ICMP	74 Echo (ping) reply id=0x0001, seq=7164/64539, ttl=55 (reques
	72	.9186850	0192.168.43.241	217.20.130.99	ICMP	74 Echo (ping) request id=0x0001, seq=7165/64795, ttl=128 (reply
	8 3	.1868980	0 217.20.130.99	192.168.43.241	ICMP	74 Echo (ping) reply id=0x0001, seq=7165/64795, ttl=55 (reques
	93	.9653270	0192.168.43.241	217.20.130.99	ICMP	74 Echo (ping) request id=0x0001, seq=7166/65051, ttl=128 (reply
1	.0 4	.2368510	0 217.20.130.99	192.168.43.241	ICMP	74 Echo (ping) reply id=0x0001, seq=7166/65051, ttl=55 (reques
1	14	.9492380	DLiteonTe_c8:30:64	ca:dd:c9:d7:d0:93	ARP	42 who has 192.168.43.1? Tell 192.168.43.241
1	.2 4	.9529820	0 ca:dd:c9:d7:d0:93	LiteonTe_c8:30:64	ARP	42 192.168.43.1 is at ca:dd:c9:d7:d0:93
	_					
Fra	me	3: 74 bvt	tes on wire (592 bit	s), 74 bytes captur	ed (592	bits) on interface 0
🕀 Eth	ern	et II. Sr	c: LiteonTe c8:30:6	4 (24:fd:52:c8:30:6	4). Dst	: ca:dd:c9:d7:d0:93 (ca:dd:c9:d7:d0:93)
Tnt	ern	et Proto	ol Version 4. Src:	192,168,43,241 (192	.168.43	.241), Dst: 217.20.130.99 (217.20.130.99)
Internet Control Message Protocol						
0000	ca	dd c9 d7	d0 93 24 fd 52 c8	30 64 08 00 45 00		.\$. R.OdE.
0010	00	3c 49 58	3 00 00 80 01 a9 57	c0 a8 2b f1 d9 14	. <ix.< td=""><td>W+</td></ix.<>	W+
0020	82	63 08 00) 31 60 00 01 1b fb	61 62 63 64 65 66	.c1	abcdef
0030	27	61 62 63	a 60 60 60 60 67 70	/1 /2 /3 /4 /5 /6	gnijk	imn opgrstuv
0040	11	01 02 03	04 03 00 07 08 09		wabcu	ergin

A sorok elején lévő + jel segítségével az egyes szinteket is alaposabban kielemezheti! (Miközben a program középső részében kijelöl valamit, az a program alsó részében is kiemelten jelenik meg.)

Milyen hosszú egy ping parancshoz tartozó keret?

Keresse meg, a vizsgált csomag feladójának fizikai címét! Melyik szinten fogja ezt keresni? Milyen címzési módot talált?

Keresse meg, hogy mi adja meg, hogy IP datagram van a vizsgált Frame-ben! Milyen értéket talált? Hány byte ez az érték?

Keresse meg, hogy milyen forrás IP címről, milyen IP célcímre ment az IP datagram. Melyik szinten fogja ezt keresni? Hány byte hosszú egy cím? Milyen TTL értéket talált?

Keresse meg, hogy mi adja meg, hogy ICMP protokoll van a vizsgált IP datagramban! Milyen értéket talált? Hány byte ez az érték?

Keresse meg, hogy mi adja meg, hogy az ICMP-ben Echo Request van! Milyen értéket talált? Hány byte ez az érték? Melyik szinten fogja ezt keresni?

Hány byte a payload az elfogott ICMP kérésben? Milyen értékűek ezek a byte-ok? Hol találta meg ezt a payloadot?

Most hasonlóan vizsgálja meg az ICMP Echo Replay-t is!

4. UDP vizsgálata







Széchenyi István Egyetem Győr Távközlési Tanszék

Vizsgálja meg az előző feladatban végrehajtott csomagelkapásban még az ICMP üzenetek előtt elkapott DNS Standard Query üzenetet! Milyen forrás fizikai címről ment a kérés? Milyen forrás IP címről, milyen cél IP címre ment a kérés?

Milyen szállítási szintű protokollt használt az DNS? Milyen érték azonosítja az UDP-t?

Hány byte egy UDP checksum? Hol találta meg?

Milyen forrásportról ment a kérés milyen célportra? Melyik szinten, hol találta meg az értékeket? Mi a DNS kérések portszáma?

Valahol megtalálta a kért nevet? (index.hu) Hol? Melyik szinten?

5. TCP vizsgálata és szűrők

Indítson egy csomagelkapást az enp11s0-án, úgy, hogy a leállítás feltétele legyen 1 perc, valamint a képernyő automatikusan gördüljön a csomagokkal. (Nem kell menteni az előző listát.) Ezután a böngészőt elindítva kérje le az *index.hu* honlapot.

A TCP protokollt a következő gyakorlaton fogjuk részletesen megismerni, most csak az első TCP szegmens tartalmát vizsgáljuk meg.

Az TCP adategységet szállító IP datagram mely mezőjének milyen értékéből derül ki, hogy a TCP protokoll adategysége utazik fölötte?

A TCP protokoll fejrészében keresse meg a cél port számát!

A hálózatokon sokszor rengeteg "minket nem érdeklő" forgalom van. Ha ezeket figyelmen kívül szeretnénk hagyni, a csomagszűrőkhöz kell nyúlnunk.

Csomagszűrők két helyen alkalmazhatók:

- 1. csomagelkapásnál
- 2. megjelenítésnél

Ha csomagelkapásánál 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 fajta szűrő szintaxisa sajnos különböző!)

A csomagelkapási beállításokon (2. gomb) belül lehet csomagszűrőket alkalmazni. (A csomagszűrési beállításokon belül több előre definiált szűrő áll rendelkezésünkre. Meg lehet adni protokollszűrést, IP cím szűrést, forrás és célport szűrést. Bővebben majd a következő gyakorlaton foglalkozunk vele.)

Most csak a megjelenítésnél használható szűrőket (Display Filter) ismerjük meg. A korábban megismert gombsor alatt a "Filter:" mezőben adjuk meg a következőt: tcp.port == 80



Széchenyi István Egyetem Győr Távközlési Tanszék

Vegyük észre, hogy gépelés közben a mező háttere zöldre vált, amikor az addig begépelt szöveg szintaktikailag helyes!

Érvényesítsük a szűrőt az Apply feliratra való kattintással.

Mit tapasztalunk?