

# Számítógépes Hálózatok

10. gyakorlat

traceroute, ping

# HÁLÓZATI ESZKÖZÖK I.

# traceroute (linux) – tracert (windows)

Cél a hálózati útvonal meghatározása egy célállomás felé!

```
lakis@dpsdk-pktgen:~$ traceroute berkeley.edu
traceroute to berkeley.edu (35.163.72.93), 30 hops max, 60 byte packets
 1 192.168.0.192 (192.168.0.192) 0.292 ms 0.344 ms 0.390 ms
 2 ikoktatok-gate.inf.elte.hu (157.181.167.254) 1.251 ms 1.250 ms 1.265 ms
 3 taurus.centaur-taurus.elte.hu (157.181.126.134) 5.180 ms 5.267 ms 5.325 ms
 4 fw1.firewall.elte.hu (157.181.141.145) 1.271 ms 1.358 ms 1.299 ms
 5 taurus.fw1.fw.backbone.elte.hu (192.153.18.146) 5.626 ms 5.356 ms 5.395 ms
 6 rtr.hbone-elte.elte.hu (157.181.141.9) 2.229 ms 1.245 ms 1.749 ms
 7 tg0-0-0-14.rtr2.vh.hbone.hu (195.111.100.47) 2.377 ms 2.415 ms 2.407 ms
 8 be1.rtr1.vh.hbone.hu (195.111.96.56) 1.945 ms 1.642 ms 1.877 ms
 9 bpt-b4-link.telia.net (80.239.195.56) 1.626 ms 1.581 ms 1.097 ms
10 win-bb2-link.telia.net (62.115.143.116) 196.574 ms win-bb2-link.telia.net (213.155.137.38) 196.993 ms
win-bb2-link.telia.net (213.155.135.222) 180.071 ms
11 ffm-bb4-link.telia.net (62.115.133.79) 199.425 ms 199.232 ms *
12 * * *
13 prs-bb3-link.telia.net (62.115.137.114) 180.494 ms 179.986 ms *
14 sjo-b21-link.telia.net (62.115.119.229) 197.252 ms 197.249 ms 197.264 ms
15 * a100row-ic-300117-sjo-b21.c.telia.net (213.248.87.118) 196.555 ms *
16 nyk-bb4-link.telia.net (62.115.142.222) 180.081 ms 54.240.242.148 (54.240.242.148) 200.986 ms
54.240.242.88 (54.240.242.88) 201.877 ms
17 54.240.242.161 (54.240.242.161) 200.935 ms * *
18 * * *
19 * * *
```

**Linuxon**

# tracert (linux) – tracert (windows)

Cél a hálózati útvonal meghatározása egy célállomás felé!

```
C:\Users\laki>tracert berkeley.edu
```

```
Tracing route to berkeley.edu [35.163.72.93]  
over a maximum of 30 hops:
```

**Windowson**

```
 1      1 ms      <1 ms      <1 ms      dlinkrouter [192.168.0.1]  
 2     24 ms      6 ms      60 ms      10.0.0.85  
 3     54 ms     18 ms     13 ms      fibhost-66-110-33.fibernet.hu [85.66.110.33]  
 4     13 ms     14 ms     13 ms      ae0.info-c1.invitech.hu [213.163.54.245]  
 5     13 ms     12 ms     17 ms      te0-0-2-3.nr11.b020698-1.bud01.atlas.cogentco.com [149.6.182.13]  
 6     13 ms     13 ms     16 ms      te0-0-2-1.agr11.bud01.atlas.cogentco.com [154.25.3.237]  
 7     15 ms     13 ms     12 ms      be3272.ccr31.bud01.atlas.cogentco.com [154.54.59.197]  
 8     17 ms     16 ms     19 ms      be3263.ccr22.bts01.atlas.cogentco.com [154.54.59.177]  
 9     22 ms     22 ms     21 ms      be3045.ccr21.prg01.atlas.cogentco.com [154.54.59.105]  
10     29 ms     30 ms     27 ms      be3027.ccr41.ham01.atlas.cogentco.com [130.117.1.205]  
11     41 ms     36 ms     41 ms      be2815.ccr41.ams03.atlas.cogentco.com [154.54.38.205]  
12    134 ms    136 ms    133 ms      be12194.ccr41.lon13.atlas.cogentco.com [154.54.56.93]  
13    133 ms    136 ms    132 ms      be2982.ccr31.bos01.atlas.cogentco.com [154.54.1.117]  
14    135 ms    134 ms    137 ms      be3599.ccr21.alb02.atlas.cogentco.com [66.28.4.237]  
15    134 ms    134 ms    135 ms      be2878.ccr21.cle04.atlas.cogentco.com [154.54.26.129]  
16    136 ms    136 ms    134 ms      be2717.ccr41.ord01.atlas.cogentco.com [154.54.6.221]  
17    148 ms    147 ms    146 ms      be2831.ccr21.mci01.atlas.cogentco.com [154.54.42.165]  
18    158 ms    159 ms    159 ms      be3035.ccr21.den01.atlas.cogentco.com [154.54.5.89]  
19    168 ms    169 ms    167 ms      be3037.ccr21.slc01.atlas.cogentco.com [154.54.41.145]  
20    183 ms    183 ms    183 ms      be3109.ccr21.sfo01.atlas.cogentco.com [154.54.44.137]  
21    186 ms    187 ms    184 ms      be3669.ccr41.sjc03.atlas.cogentco.com [154.54.43.10]  
22    184 ms    186 ms    185 ms      38.88.224.218  
23      *         *         *         Request timed out.  
24      *         *         *         Request timed out.  
25      *         *         *         Request timed out.
```

# Ping a hoszt elérhetőségének ellenőrzésére és a Round Trip Time (RTT) méréséhez

## Linuxon

```
lakis@dpsdk-pktgen:~$ ping -c 3 berkeley.edu
PING berkeley.edu (35.163.72.93) 56(84) bytes of data.
64 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=1 ttl=23 time=194 ms
64 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=2 ttl=23 time=194 ms
64 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=3 ttl=23 time=193 ms

--- berkeley.edu ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 193.093/193.937/194.428/0.786 ms
```

# Ping a hoszt elérhetőségének ellenőrzésére és a Round Trip Time (RTT) méréséhez

## Windowson

```
C:\Users\laki>ping -n 3 berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 32 bytes of data:
Reply from 35.163.72.93: bytes=32 time=200ms TTL=39
Reply from 35.163.72.93: bytes=32 time=201ms TTL=39
Reply from 35.163.72.93: bytes=32 time=200ms TTL=39

Ping statistics for 35.163.72.93:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 200ms, Maximum = 201ms, Average = 200ms
```

# NC-NetCat (SoCat), avagy hálózati svájcbicska

# szerver imitálása

```
nc -l -p 1234
```

# kliens imitálása

```
nc destination_host 1234
```

NetCat TUTORIAL:

<https://www.binarytides.com/netcat-tutorial-for-beginners>

SoCat TUTORIAL:

<https://blog.rootshell.be/2010/10/31/socat-another-network-swiss-armyknife>

# Tcpdump – hálózati forgalomfigyelés

```
lakis@dpedk-switch:~$ sudo tcpdump -i enp8s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp8s0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:15:26.376139 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 4154664816:4154665024, ack 289117644, win 384, length 208
09:15:26.376403 IP 192.168.0.102.43549 > 192.168.0.192.domain: 52681+ PTR? 35.167.181.157.in-addr.arpa. (45)
09:15:26.376994 IP 192.168.0.192.domain > 192.168.0.102.43549: 52681* 1/0/0 PTR oktnb35.inf.elte.hu. (78)
09:15:26.377100 IP 192.168.0.102.57511 > 192.168.0.192.domain: 64457+ PTR? 102.0.168.192.in-addr.arpa. (44)
09:15:26.377645 IP 192.168.0.192.domain > 192.168.0.102.57511: 64457 NXDomain 0/1/0 (79)
09:15:26.377723 IP 192.168.0.102.49012 > 192.168.0.192.domain: 6981+ PTR? 192.0.168.192.in-addr.arpa. (44)
09:15:26.377851 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 208:400, ack 1, win 384, length 192
09:15:26.378180 IP 192.168.0.192.domain > 192.168.0.102.49012: 6981 NXDomain 0/1/0 (79)
09:15:26.378267 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 400:976, ack 1, win 384, length 576
09:15:26.378291 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 976:1248, ack 1, win 384, length 272
09:15:26.378340 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 1248:1600, ack 1, win 384, length 352
09:15:26.378387 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 1600:1776, ack 1, win 384, length 176
09:15:26.378440 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 1776:1952, ack 1, win 384, length 176
09:15:26.378489 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 1952:2128, ack 1, win 384, length 176
09:15:26.378538 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 2128:2304, ack 1, win 384, length 176
09:15:26.378587 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 2304:2480, ack 1, win 384, length 176
09:15:26.378636 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 2480:2656, ack 1, win 384, length 176
09:15:26.378685 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 2656:2832, ack 1, win 384, length 176
09:15:26.378734 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 2832:3008, ack 1, win 384, length 176
09:15:26.378783 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 3008:3184, ack 1, win 384, length 176
09:15:26.378832 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 3184:3360, ack 1, win 384, length 176
```

## Protokol szűrés

```
lakis@dpedk-switch:~$ sudo tcpdump -i enp8s0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp8s0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:16:49.470737 IP dpdk-pktgen > 192.168.0.102: ICMP echo request, id 5668, seq 1, length 64
09:16:49.470766 IP 192.168.0.102 > dpdk-pktgen: ICMP echo reply, id 5668, seq 1, length 64
09:16:50.471818 IP dpdk-pktgen > 192.168.0.102: ICMP echo request, id 5668, seq 2, length 64
09:16:50.471834 IP 192.168.0.102 > dpdk-pktgen: ICMP echo reply, id 5668, seq 2, length 64
09:16:51.471716 IP dpdk-pktgen > 192.168.0.102: ICMP echo request, id 5668, seq 3, length 64
09:16:51.471732 IP 192.168.0.102 > dpdk-pktgen: ICMP echo reply, id 5668, seq 3, length 64
09:16:52.471713 IP dpdk-pktgen > 192.168.0.102: ICMP echo request, id 5668, seq 4, length 64
09:16:52.471729 IP 192.168.0.102 > dpdk-pktgen: ICMP echo reply, id 5668, seq 4, length 64
09:16:53.471720 IP dpdk-pktgen > 192.168.0.102: ICMP echo request, id 5668, seq 5, length 64
09:16:53.471736 IP 192.168.0.102 > dpdk-pktgen: ICMP echo reply, id 5668, seq 5, length 64
```



# Tcpdump – hálózati forgalomfigyelés

## host és port szűrés

```
lakis@dppk-switch:~$ sudo tcpdump -i enp8s0 host 192.168.0.101 and port 1111
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp8s0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:20:23.289035 IP dpdk-pktgen.48524 > 192.168.0.102.1111: Flags [S], seq 1544265047, win 29200, options [mss 1460,sackOK,TS v
length 0
09:20:23.289067 IP 192.168.0.102.1111 > dpdk-pktgen.48524: Flags [R.], seq 0, ack 1544265048, win 0, length 0
```

## Mentés pcap fileba

```
lakis@dppk-switch:~$ sudo tcpdump -w test.pcap -i enp8s0
tcpdump: listening on enp8s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4 packets captured
6 packets received by filter
0 packets dropped by kernel
lakis@dppk-switch:~$ tcpdump -r test.pcap
reading from file test.pcap, link-type EN10MB (Ethernet)
09:31:32.000164 IP 192.168.0.102.ssh > oktnb35.inf.elte.hu.55015: Flags [P.], seq 4154857792:4154857936, ack 289145644, win 384, length 144
09:31:32.060031 IP oktnb35.inf.elte.hu.55015 > 192.168.0.102.ssh: Flags [.], ack 144, win 3542, length 0
09:31:34.354029 IP 192.168.0.192.48309 > 255.255.255.255.7437: UDP, length 173
09:31:37.377992 IP 192.168.0.192.48309 > 255.255.255.255.7437: UDP, length 173
```

# Wireshark

The screenshot displays the Wireshark Network Analyzer interface. The title bar reads "The Wireshark Network Analyzer [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, search, and analysis. Below the toolbar is a filter bar with a dropdown menu set to "Expression..." and buttons for "Clear", "Apply", and "Save".

The main content area is divided into three columns:

- Capture:** Contains sections for "Interface List" (Live list of the capture interfaces), "Start" (Choose one or more interfaces to capture from, then Start), and "Capture Options" (Start a capture with detailed options). Below this is a "Capture Help" section with "How to Capture" and "Network Media".
- Files:** Contains an "Open" section (Open a previously captured file) and "Open Recent:" with two entries: "C:\Users\ge-sar\Desktop\captured\simple\01-centerpoints-0-0.pcap (24 kB)" and "C:\Users\ge-sar\Desktop\example output\01-centerpoints-0-0.pcap (40 kB)". It also has a "Sample Captures" section (A rich assortment of example capture files on the wiki).
- Online:** Contains sections for "Website" (Visit the project's website), "User's Guide" (The User's Guide (local version, if installed)), and "Security" (Work with Wireshark as securely as possible).

The status bar at the bottom shows "Ready to load or capture", "No Packets", and "Profile: Default".

# Wireshark

01-centerpoints-0-0.pcap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.17	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
2	0.029669	10.1.1.1	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
3	0.048943	10.1.1.37	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
4	0.131429	10.1.1.18	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
5	0.133386	10.1.1.21	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
6	0.210913	10.1.1.25	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
7	0.318007	10.1.1.3	10.1.1.255	OLSR v1	84	OLSR (IPv4) Packet, Length: 20 Bytes
8	1.918582	10.1.1.21	10.1.1.255	OLSR v1	156	OLSR (IPv4) Packet, Length: 92 Bytes
9	1.961619	10.1.1.37	10.1.1.255	OLSR v1	172	OLSR (IPv4) Packet, Length: 108 Bytes
10	2.146770	10.1.1.18	10.1.1.255	OLSR v1	180	OLSR (IPv4) Packet, Length: 116 Bytes
11	2.220068	10.1.1.25	10.1.1.255	OLSR v1	148	OLSR (IPv4) Packet, Length: 84 Bytes
12	2.284430	10.1.1.3	10.1.1.255	OLSR v1	116	OLSR (IPv4) Packet, Length: 52 Bytes
13	2.309605	10.1.1.17	10.1.1.255	OLSR v1	156	OLSR (IPv4) Packet, Length: 92 Bytes
14	2.240700	10.1.1.1	10.1.1.255	OLSR v1	132	OLSR (IPv4) Packet, Length: 68 Bytes

Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)  
IEEE 802.11 Data, Flags: o.....  
Logical-Link Control  
Internet Protocol Version 4, Src: 10.1.1.17 (10.1.1.17), Dst: 10.1.1.255 (10.1.1.255)  
User Datagram Protocol, Src Port: 698 (698), Dst Port: 698 (698)  
Optimized Link State Routing Protocol

```
0000 08 80 00 00 ff ff ff ff ff 00 00 00 00 11 .....  
0010 00 00 00 00 00 11 00 00 aa aa 03 00 00 00 08 00 .....  
0020 45 00 00 30 00 00 00 00 40 11 00 00 0a 01 01 11 E..O...@.....  
0030 0a 01 01 ff 02 ba 02 ba 00 1c 00 00 00 14 00 00 .....  
0040 01 86 00 10 0a 01 01 11 01 00 00 00 00 05 03 .....  
0050 00 00 00 00 .....
```

File: "C:\Users\ge-sar\Desktop\egyetem\nw... Packets: 218 · Displayed: 218 (100.0%) · Load time: 0:00:00.4 Profile: Default

Szűrők definiálására  
alkalmas input eszközök

Csomag összefoglaló  
nézete

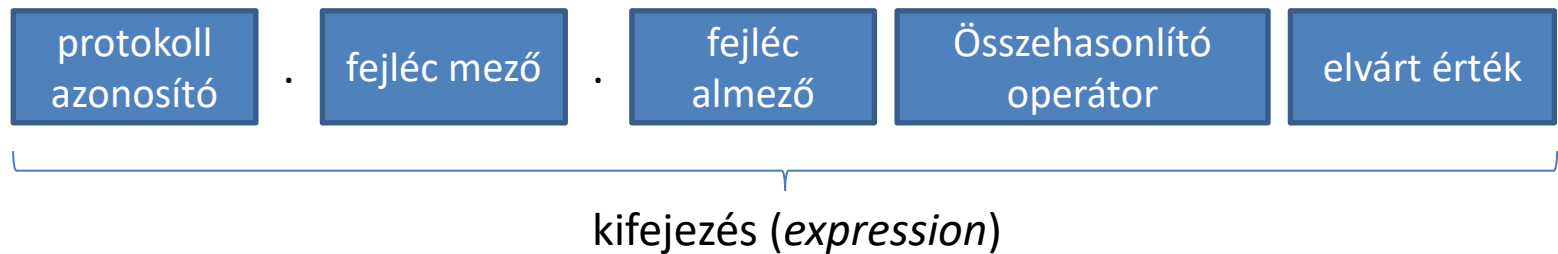
Kiválasztott csomag  
hierarchikus nézet

Kiválasztott csomag bájttól  
alapú nézet

Szűrés statisztikái

# Wireshark

- Korábban rögzített adatok elemzésére szolgál.
- Szűrés felépítése:



- Operátorok: or, and, xor, not
- Példa: `tcp.flags.ack==1 and tcp.dstport==80`

# Szűrési feladatok 1 - HTTP

A [http\\_out.pcapng](#) felhasználásával állomány felhasználásával válaszolja meg az alábbi kérdéseket:

1. Milyen oldalakat kértek le a szűrés alapján? Milyen böngészőt használtak hozzá?
2. Hány darab képet érintett a böngészés? (Segítség: *webp.*)
3. Hány olyan erőforrás volt, amelyet nem kellett újra töltenie a böngészőnek? Mely oldalakat érintette ez?
4. Volt-e olyan kérés, amely titkosított kommunikációt takar? (Segítség: *SSL/TLS.*) Kövesse végig az első TCP folyamat. Mit tud kideríteni a kommunikációról?

# Szűrési feladatok 1 - HTTP

A `http_out.pcapng` felhasználásával állomány felhasználásával válaszolja meg az alábbi kérdéseket:

1. Milyen oldalakat kértek le a szűrés alapján? Milyen böngészőt használtak hozzá?
  - `http.request.method=="GET"`
2. Hány darab képet érintett a böngészés?
  - `http.accept == "image/webp,*/*;q=0.8"`
3. Hány olyan erőforrás volt, amelyet nem kellett újra töltenie a böngészőnek? Mely oldalakat érintette ez?
  - `http.response.code == 304` (to.ttk.elte.hu és www.inf.elte.hu)
4. Volt-e olyan kérés, amely titkosított kommunikációt takar? (Segítség: *SSL/TLS*.) Kövesse végig az első TCP folyamatát. Mit tud kideríteni a kommunikációról?
  - `tcp.dstport==443`

# Szűrési feladatok 2 - DNS

- A `dns_out.pcapng` felhasználásával állomány felhasználásával válaszolja meg az alábbi kérdéseket:
  1. Hány domén név feloldást kezdeményeztek a szűrés alapján? Mely domén nevek voltak ezek?
  2. Válaszon ki 3 darab különböző domén nevet, és keresse meg a válasz csomagokat hozzájuk? Hány darab válasz van az egyes kérésekre? (Segítség: *ID.*)
  3. Hány olyan névfeloldás volt, amelyre több válasz is érkezett?
  4. Volt-e iteratív lekérdezés a szűrésben? Ha igen, akkor mennyi? Ha nem, akkor mi lehet a magyarázat?

# Szűrési feladatok 3 - NEPTUN

- A `neptun_out.pcapng` felhasználásával állomány felhasználásával válaszolja meg az alábbi kérdéseket:
  1. Milyen oldalakat kértek le a szűrés alapján? Milyen böngészőt használtak hozzá?
  2. Hány darab `SSL/TLS` protokollt használó csomag van? Az elsőt kövesse végig a kommunikációt. Minden működési elvnek megfelelően lezajlott?
  3. Kezdeményezett-e megszakítást a szerver a kommunikáció során?
  4. Kideríthető-e, hogy milyen kommunikáció folyt a szerver és a kliens között? Esetleg megtippelhető-e a használt böngésző típusa?



**VÉGE**