Számítógépes Hálózatok

10. gyakorlat

traceroute, ping

HÁLÓZATI ESZKÖZÖK I.

traceroute (linux) – tracert (windows)

Cél a hálózati útvonal meghatározása egy célállomás felé!

```
lakis@dpdk-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

traceroute (linux) – tracert (windows)

Cél a hálózati útvonal meghatározása egy célállomás felé!

Windowson

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

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

  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@dpdk-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 svájcibicska

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@dpdk-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@dpdk-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

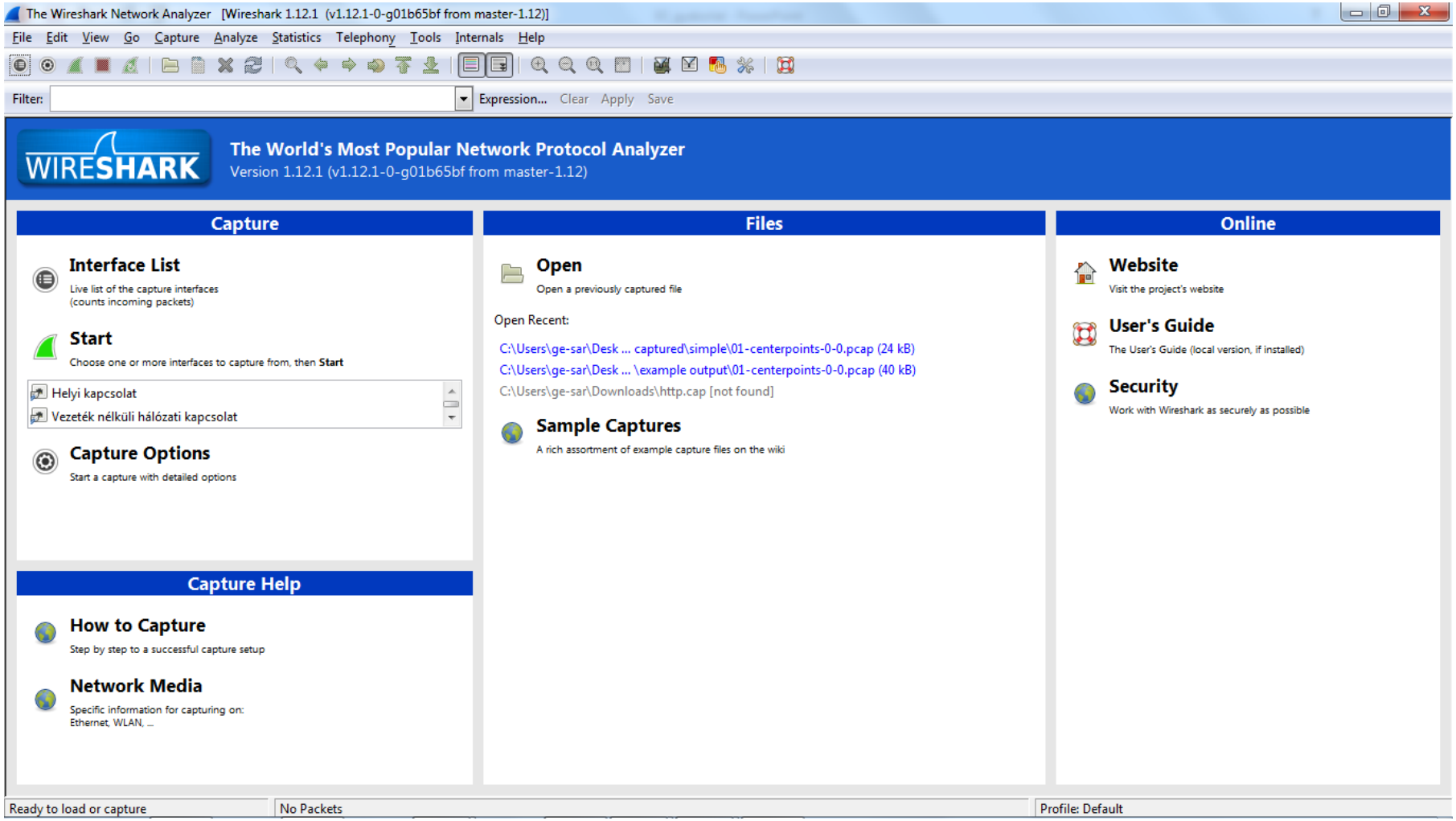
host és port szűrés

```
lakis@dpdk-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
```

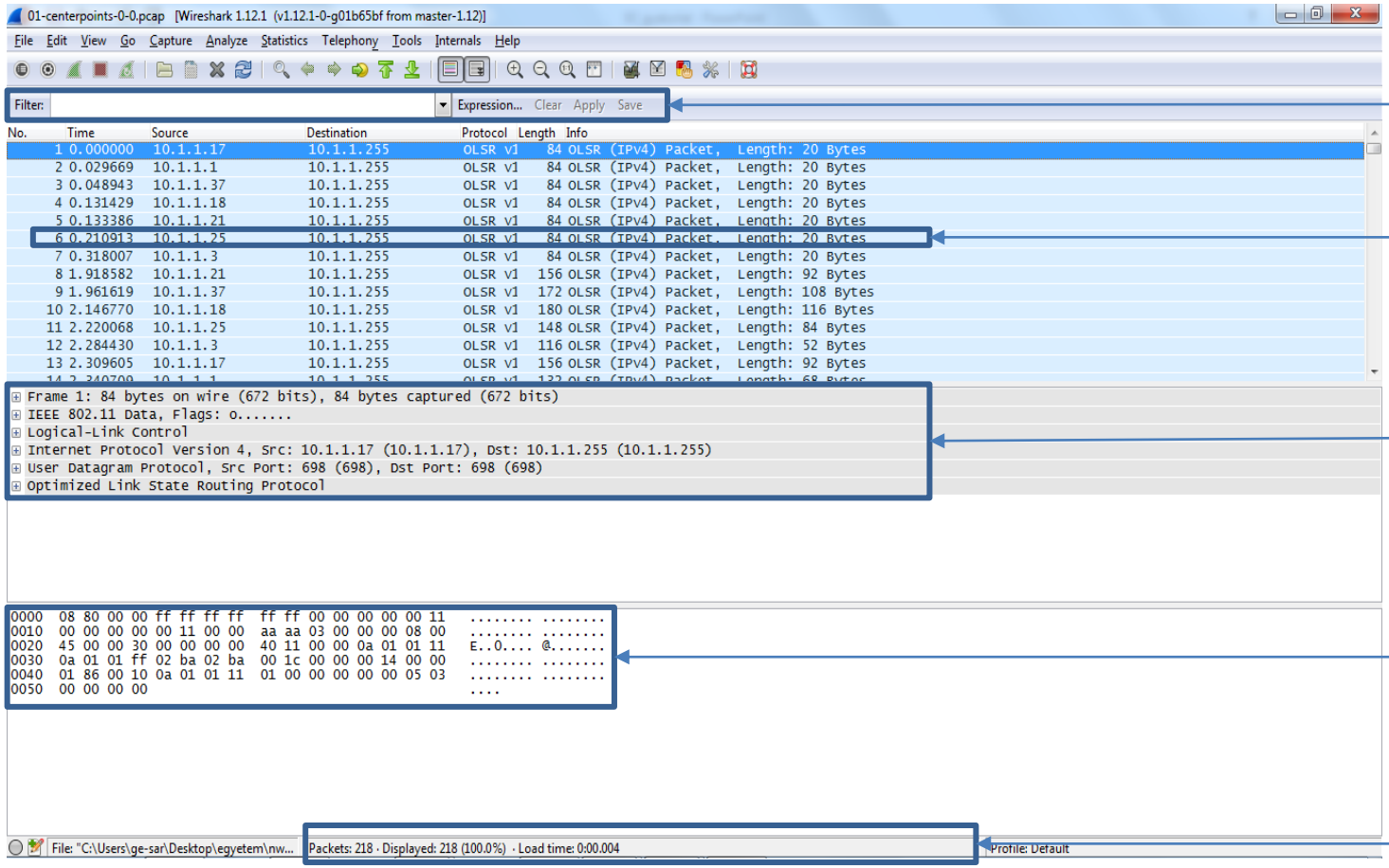
Mentés pcap fileba

```
lakis@dpdk-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@dpdk-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 Wireshark Network Analyzer [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
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Helyi kapcsolat
Vezeték nélküli hálózati kapcsolat
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
C:\Users\ge-sar\Desk ... captured\simple\01-centerpoints-0-0.pcap (24 kB)
C:\Users\ge-sar\Desk ... \example output\01-centerpoints-0-0.pcap (40 kB)
C:\Users\ge-sar\Downloads\http.cap [not found]
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

Wireshark



Szűrők definiálására alkalmas input eszközök

Csomag összefoglaló nézete

Kiválasztott csomag hierarchikus nézet

Kiválasztott csomag bájt-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 folyamát. 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 folyamát. 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 elsőn 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?

HTTP vs HTTPS

- Nyissuk meg a sample3.pcapng fájlt!
- Keressük olyan POST kérést, amely login oldalra vezet!
- Nézzük meg a POST hívás paramétereit!

VÉGE