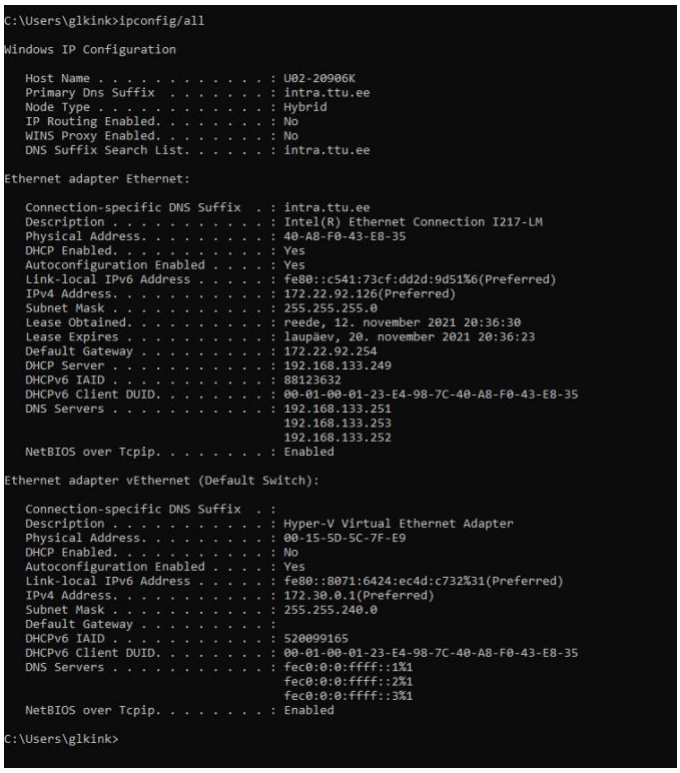
IEE1220 Side arvutivõrgu protokollid labori aruanne

Töö tegija nimi:Glen Kink

Töö tegemise kuupäev:16.11.2021

4.2 Arvuti IP aadress



A. Enda arvuti MAC aadress käsurealt vaadates: 40-A8-F0-43-E8-35

B. Enda arvuti IP aadress käsurealt vaadates: 172.22.92.126
Enda arvuti IPv6 aadress käsurealt vaadates: fe80::c541:73cf:dd2d:9d51%6

C. Oma võrgu marsruuteri IP aadress (Default Gateway): 172.22.92.254

D. Nimeserverite IP aadressid (DNS servers): 192.168.133.251

192.168.133.253

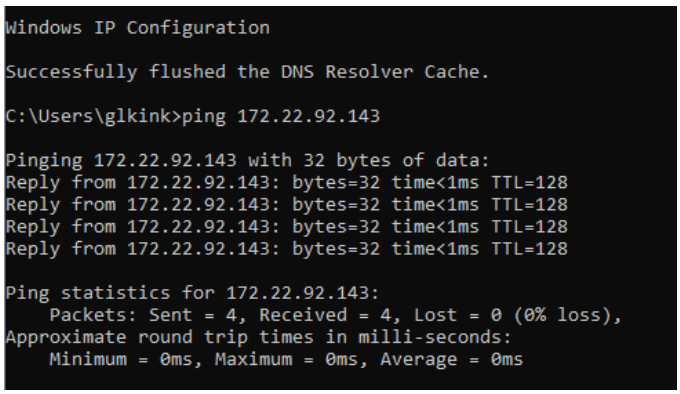
192.168.133.252

E. Veebilehel näidatud enda arvuti IP aadress: 172.30.0.1

F. Mis on võimalike erinevuste põhjuseks? ipconfig käsk näitab sisevõrgu IP aadressi, veebileht aga välisvõrgu aadressi.

4.3 Ping (protokollid ARP, ICMP, UDP, DNS)

Salvestada käsurea aken koos ping tulemustega.



A. Mida programm ping teeb ja mida tulemus näitab? Ping mõõdab lähtehostilt sihtarvutisse saadetud sõnumite edasi-tagasi aega, mis kajatakse tagasi allikale.

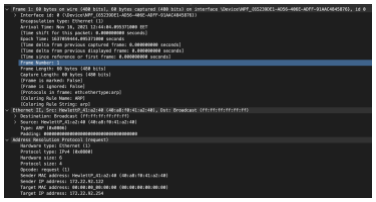
ARP

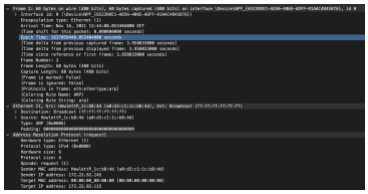
B. Milliste protokollide päiseid ARP paketid sisaldavad? Aadressiteisenduse protokoll (inglise Address Resolution Protocol, lühend ARP) on protokoll IP-aadressi vastendamiseks riistvara aadressi ehk MAC-aadressiga. Protocols in frame: eth:ethertype:arp

C. Millisele aadressile saadetakse ARP päring? Dst: Broadcast (ff:ff:ff:ff:ff:ff)

D. Milliselt aadressilt tuleb ARP vastus? Source: HewlettP 41:a2:40 (40:a8:0:41:22:40)

E. Milline on ARP pakettide sisu? ARP päringu pakett sisaldab lähte-MAC-aadressi ja lähte-IP-aadressi ning sihtkoha IP-aadressi. Iga kohaliku võrgu host saab selle paketi.





Lisada ekraanipilt Wiresharki keskmisest aknast, kus näha dekodeeritud kujul ARP päringu paketis EthernetII ja ARP osa ning teine ekraanipilt Wiresharki keskmisest aknast, kus näha ARP vastuse paketis dekodeeritud EthernetII ja ARP osa.

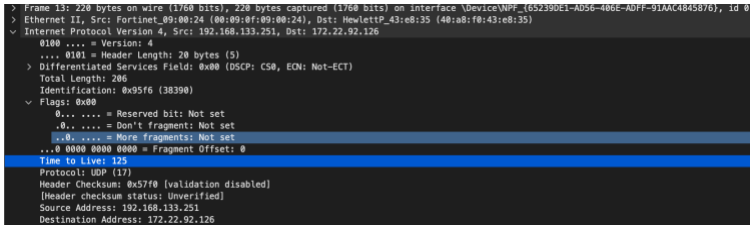
IP

F. Milline väärtus on väljal Flags ja millist informatsiooni see annab? Flags: 0x00
0... .... = Reserved bit: Not set Kui see on 1 pannakse üks bitt kõrvale kui tulevikus protokollil vaja on.
.0.. .... = Don't fragment: Not set Kui see on 1 ja IP peab paketi killustama ehk omakorda pakettideks jagama, siis IP viskab paketi minema killustamise asemel.
..0. .... = More fragments: Not set Kui see on 0, tähendab et rohkem andmekilde (pakette) ei tule.

G. Milline väärtus on väljal Header Length ja millist informatsiooni see annab? .... 0101 = Header Length: 20 bytes (5)
Näitab mitu 32 bitist sõna on päises. 32/8= 4 baiti 4*5= 20 baiti. Praegusel juhul ütleb, et päise pikkus on 20 baiti ehk 5 nelja baidist sõna. Päis on alati vähemalt 20 baiti.

H. Milline väärtus on väljal Total Length ja millist informatsiooni see annab? Total Length: 206
Näitab kogu andmemahu suurust ehk praegu 206 baiti.

I. Milline väärtus on väljal Protocol ja millist informatsiooni see annab? Protocol: UDP (17)
Kasutajadatagrammi protokoll (ingl User Datagram Protocol, UDP) on transpordikihi andmesideprotokoll, mis on defineeritud IPga sõnumite saatmiseks ehk näitab IP-le kuhu paketid saata.



Lisada ekraanipilt ühest paketist (ping vastus) Wiresharki keskmises aknas, kus IP osa on tervenisti lahti koos välja Flags sisuga.

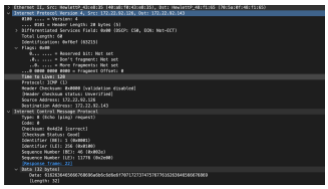
ICMP

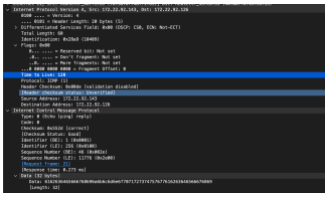
J. Milliste protokollide päiseid ICMP paketid sisaldavad? Protocols in frame: eth:ethertype:ip:icmp:data

K. Millisele aadressile saadetakse ping päring (MAC aadress ja IP aadress)? (MAC aadress ja IP aadress)?
MAC: (40:a8:f0:43:8:35) IP: 172.22.92.126

L. Milliselt aadressilt tuleb vastus (MAC aadress ja IP aadress)? MAC: 00:09:0f:fb:74:1c IP: 172.22.92.143

M. Mis on päringu ja vastuse Data osas (kirjeldada oma sõnadega andmete kogust ja sisu)?
andmekogus on 32 baiti ja sisu on numbrid ja tähed, kust täpitähed puuduvad.

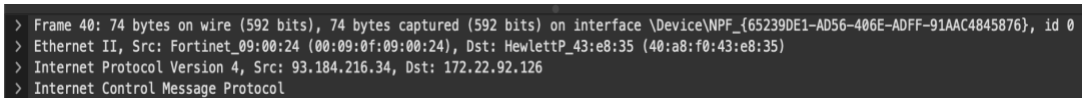




Lisada ekraanipildid ping päringu ja ping vastuse Wiresharki keskmisest aknast, kus dekodeeritud ICMP paketi IP ja ICMP osa.

N. Millisele aadressile saadetakse ping päring (MAC aadress ja IP aadress)?
MAC: 00:09:0f:09:00:24
IP: 93.184.216.34

O. Milliselt aadressilt tuleb vastus (MAC aadress ja IP aadress)? MAC: 00:09:0f:fb:74:1c
IP: 93.184.216.34



Lisada ekraanipilt ping päringu ja ping vastuse pakettidest Wiresharki keskmises aknas, (kus kõik plussid kinni).

UDP, DNS

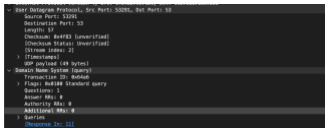
P. Milliste protokollide päiseid DNS paketid sisaldavad? Protocols in frame: eth:ethertype:ip:udp:dns

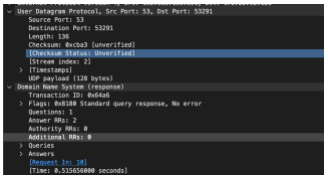
R. Kui pikk on UDP päis? 8 baiti

S. Mis sisaldub UDP päises? User Datagram Protocol, päringu saatva IP aadressi port, päringu vastuvõtva IP aadressi port

T. Milline on UDP pordi number DNS jaoks (serveri port)? 53

U. Mis sisaldub DNS osas? Transaction ID, Flags, Queries





Lisada ekraanipildid DNS päringu ja vastuse pakettidest Wiresharki keskmises aknas, kus UDP ja DNS osad on lahti.

4.4 Traceroute

```
C:\Users\glkink>tracert www.example.com

Tracing route to www.example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.22.92.254
  2     *        *        *     Request timed out.
  3     1 ms     1 ms     1 ms  ttu-gw.eenet.ee [193.40.244.1]
  4     2 ms     2 ms     2 ms  fi-csc2.nordu.net [109.105.98.113]
  5    17 ms    17 ms    17 ms  de-hmb.nordu.net [109.105.97.77]
  6    24 ms    24 ms    24 ms  nl-sar.nordu.net [109.105.97.51]
  7    24 ms    24 ms    29 ms  nl-ams.nordu.net [109.105.97.217]
  8   108 ms   108 ms   108 ms  us-man.nordu.net [109.105.97.64]
  9   100 ms   108 ms   100 ms  edgecast.com [198.32.160.14]
 10   101 ms   102 ms   101 ms  ae-66.core1.nyb.edgecastcdn.net [152.195.69.131]
 11   100 ms   100 ms   100 ms  93.184.216.34

Trace complete.
```

Lisada ekraanipilt käsurealt olevatest traceroute tulemustest.

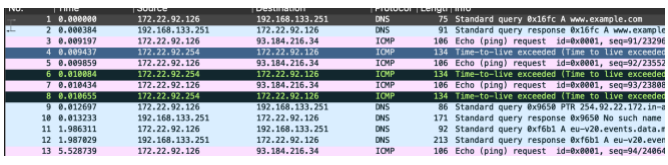
A. Mis on traceroute tulemuseks üldiselt? Enamik rakendusi sisaldab vähemalt valikuid, et määrata ühe hüppe kohta saadetavate päringute arv, vastuse ootamise aeg, vaheldumislimiit ja kasutatava port. Määramata suvanditeta traceroute'i kutsumine kuvab saadaolevate valikute loendi, samas kui man traceroute pakub rohkem üksikasju, sealhulgas kuvatud vealipud. Näitab mis marsruuterist pakett läbi läks ja kaua tal läks aega.

B. Mitme marsruuteri kaugusel meie võrgust asub www.example.com? 9 äkki

C. Milliseid protokolle kasutatakse tracert käsu täitmiseks? ICMP, DNS

D. Milline paketi eluaja (Time To Live, TTL) väärtus on kõikidel ICMP päringu pakettidel ning vastuse pakettidel? Päringu pakettidel 91, vastuste pakketidel 134.

E. Mida TTL näitab? Näitab kaua pakette hoitakse enne kui need kustutatakse.

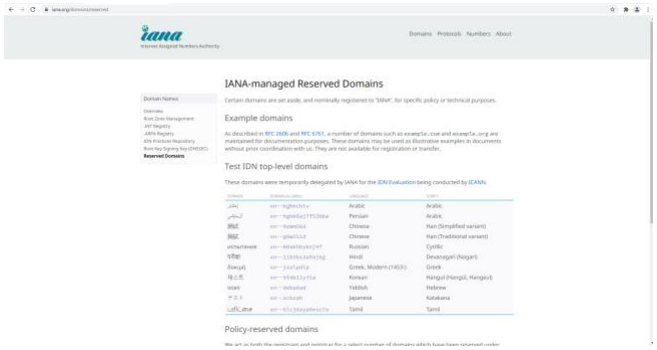


Lisada Wiresharki ülemise akna ekraanipilt koos kõikidest traceroutega seotud pakettidest.

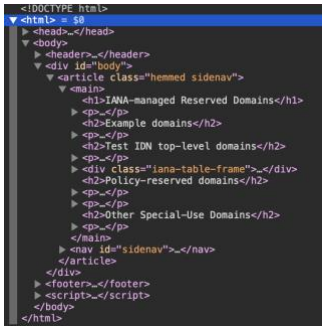
4.5 WWW (protokollid TCP, HTTP)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.22.92.126	93.184.216.34	TCP	66	60044 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
2	0.001430	172.22.92.126	93.184.216.34	TCP	66	60045 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
3	0.091018	93.184.216.34	172.22.92.126	TCP	66	80 → 60044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
4	0.091107	172.22.92.126	93.184.216.34	TCP	54	60044 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5	0.091433	172.22.92.126	93.184.216.34	HTTP	487	GET / HTTP/1.1
6	0.092542	93.184.216.34	172.22.92.126	TCP	66	80 → 60045 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
7	0.092652	172.22.92.126	93.184.216.34	TCP	54	60045 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8	0.182477	93.184.216.34	172.22.92.126	TCP	60	80 → 60044 [ACK] Seq=1 Ack=434 Win=67072 Len=0
9	0.182947	93.184.216.34	172.22.92.126	HTTP	1081	HTTP/1.1 200 OK (text/html)
10	0.224103	172.22.92.126	93.184.216.34	TCP	54	60044 → 80 [ACK] Seq=434 Ack=1028 Win=261632 Len=0

Lisada Wiresharki ülemisest aknast ekraanipilt.



Lisada ekraanipilt külastatud veebilehest.



Lisada salvestatud lehe lähtekood.

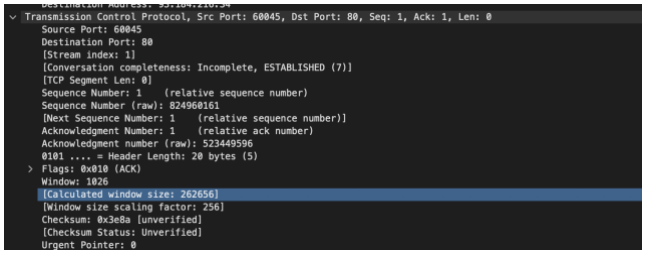
A. Milliste protokollide päiseid saadud paketid sisaldavad? TCP, HTTP

B. Kui pikk on TCP päis? 32 baiti

C. Millised väärtused on väljadel Sequence Number ja Acknowledgement number ja millist informatsiooni see annab? 0 ja 0. See näitab, et valisin esimese paketi - pakett on teele saadetud aga pole veel vastu võetud. Järgmine pakett näitaks 0 ja 1, mis tähendab et pakett saadi kätte. Järjenumber on saadetud TCP-paketi (nimetatakse ka TCP segmendiks) andmete esimese baidi baidinumber. Kinnitusnumber on järgmise baidi järjenumber, mille vastuvõtja ootab. Kinnitusnumber kehtib ainult siis, kui ACK-lipp on üks.

D. Kuidas TCP ühendust alustatakse (3 esimest paketti - milline arvuti millisele saadab ja millised TCP lipud on aktiveeritud)? Lipud aktiveeritud : 1) [SYN], 2) [SYN] , [ACK] 3) [ACK]
ehk esimene arvuti teisele, teine esimesele ja esimene uuesti teisele

E. Kuidas TCP ühendust lõpetatakse (4 viimast paketti - milline arvuti millisele saadab ja millised TCP lipud on aktiveeritud)? Lipud aktiveeritud : 1) [FIN], [ACK] 2) [ACK] 3) [FIN], [ACK] 4) [ACK]
ehk teiselt arvutilt esimesele, esimeselt teisele, esimeselt uuesti teisele ja lõpuks teiselt esimesele arvutile.



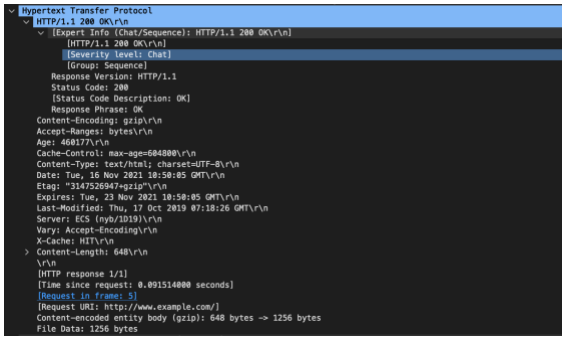
Lisada Wiresharki ekraanipilt ühest paketist, kus keskmises aknas on TCP osa lahti.

HTTP

F. Milline HTTP päring saadetakse (järgmine pakett, mille Teie arvuti saatis pärast TCP ühenduse loomist)? GET / HTTP/1.1

G. Milline tuleb HTTP vastus sellele päringule? HTTP/1.1 200 OK (text/html)

H. Milline on TCP pordi number HTTP jaoks (serveri port)? Destination Port: 80



Lisada ekraanipilt päringu paketist Wiresharki akna keskmine osa, kus HTTP osa on lahti ning vastuse paketist Wiresharki akna keskmine osa, kus HTTP osa on lahti.

4.6 Individuaalülesanne

Lähteandmete kogumine

Lisada ekraanipilt ping käsureast ja tulemustest.

Üliõpilaskood: 213427IACB

Ping käsurida: ping -s 1900 www.example.com -t 10

Keskmine RTT:128ms

Wiresharkist leida:

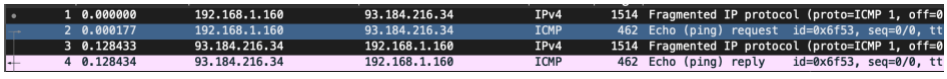
mitmes fragmendis etteantud pikkusega üks ping päring saadeti:

ühe päringu andmete (data) osa pikkus (kõikides fragmentides kokku): 1514

EthernetII päise pikkus:2

IP päise pikkus:4

ICMP päise pikkus:1



Lisada Wiresharki ekraanipilt, kus peal ülemises aknas üks päring koos fragmentidega ja üks vastus fragmentidega (iga pakett on üks rida).

LISADA ÜLESANDE LAHENDUSKÄIK JA TULEMUSED!!

Kasulikud andmed: 1900baiti = 15 200 bitti
Edastatud andmed: 1908 baiti
Kulunud aeg: 128 ms = 0,128 s
Edastuskiirus = 15200 / 0,064 = 237.5kbit/s

Efektiivsus = 1900/1908*100 = 99,6%

Kokkuvõte ja järeldused

KIRJUTA KOKKUVÕTE JA JÄRELDUSED SIIA!

Õppisin laboris kasutama Wiresharki ning arvutivõrgu protokollidest õppisin ka omajagu juurde. Labor oli põnev, aga aruannet oli väga raske kirjutada, kuid üldmulje oli hea. Õppejõud oli super nagu alati.