Wireshark Gruppe 4

Julian Mennel, Maximilian Schmidt

1.

-UDP

-ARP

-SSDP

-DHCPv6

-TCP+

-DNS

-ICMP

2.

0.916093-0.818336 = 100ms

3.

Source:

IP: 141.37.168.38

MAC: 90:1b:0e:f1:7a:f9

Destination:

IP: 128.119.245.12

MAC: 34:17:eb:46:9e:02

Abhängig von gets und responds gleichen sich die MAC-Adressen.

4.

Ethernet2	DataLink
IPv4	Network
TCP	Transport
HTTP	Application

Aufgabe 4:

1.Ethernet 2.IP 3. TCP 4. Rest HTP

0000 |38 22 d6 67 19 00 00 21 cc 63 82 2c 08 00| 45 00 8".g...!.c.,..E.

0010 02 9c 02 ed 40 00 80 06 40 66 8d 25 1d 5d 5b c6 ....@...@f.%.][.

0020 ae c0| e2 26 00 50 4f 4c 29 24 72 ce 3c d4 50 18 ...&.POL)$r.<.P.

0030 40 b0 62 e7 00 00| 47 45 54 20 2f 77 69 6b 69 2f @.b...GET /wiki/

0040 53 69 6d 70 6c 65 5f 53 65 72 76 69 63 65 5f 44 Simple_Service_D

0050 69 73 63 6f 76 65 72 79 5f 50 72 6f 74 6f 63 6f iscovery_Protoco

0060 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 l HTTP/1.1..Host

0070 3a 20 64 65 2e 77 69 6b 69 70 65 64 69 61 2e 6f : de.wikipedia.o

0080 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 rg..User-Agent:

0090 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/5.0 (Win

00a0 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 dows NT 6.1; WOW

00b0 36 34 3b 20 72 76 3a 33 32 2e 30 29 20 47 65 63 64; rv:32.0) Gec

MAC-Dest: 38:22:d6:67:19:00

MAC-Source: 00:21:cc:63:82:2c

IP-Source: 8d 25 1d 5d = 141.37.29.93

IP-Dest:5b c6 ae c0 = 91.198.174.192

SourcePort: e2 26 = 57894

DestPort: 80

Aufgabe5:

1. http && tcp.port==80

2. In dem fall ja, jedoch ist es nicht immer so.

3. http && !(udp.port==1900) gibt an, dass kein udp-Port mit der nummer 1900 in der suche herauskommt.

4. ip.src==ip.dst

Aufgabe6:

Upstream: 229 Pakete * 136.42 Bytes = 31240.18 Bytes

Downstream: 427 Pakete * 1122.6 Bytes = 479350.2 Bytes

3. 11 unterschiedliche

4. 11-13 sockets

Aufgabe7:

Pakete im downstream haben eine periodische Datenrate. Pakete kommen in gleichmäßigen Abständen an.

Pakete im upstream sind unregelmäßig und wesentlich kleiner, hier werden requests gestellt, währen in den relativ großen Paketen des downstreams,

die Daten gesendet werden.