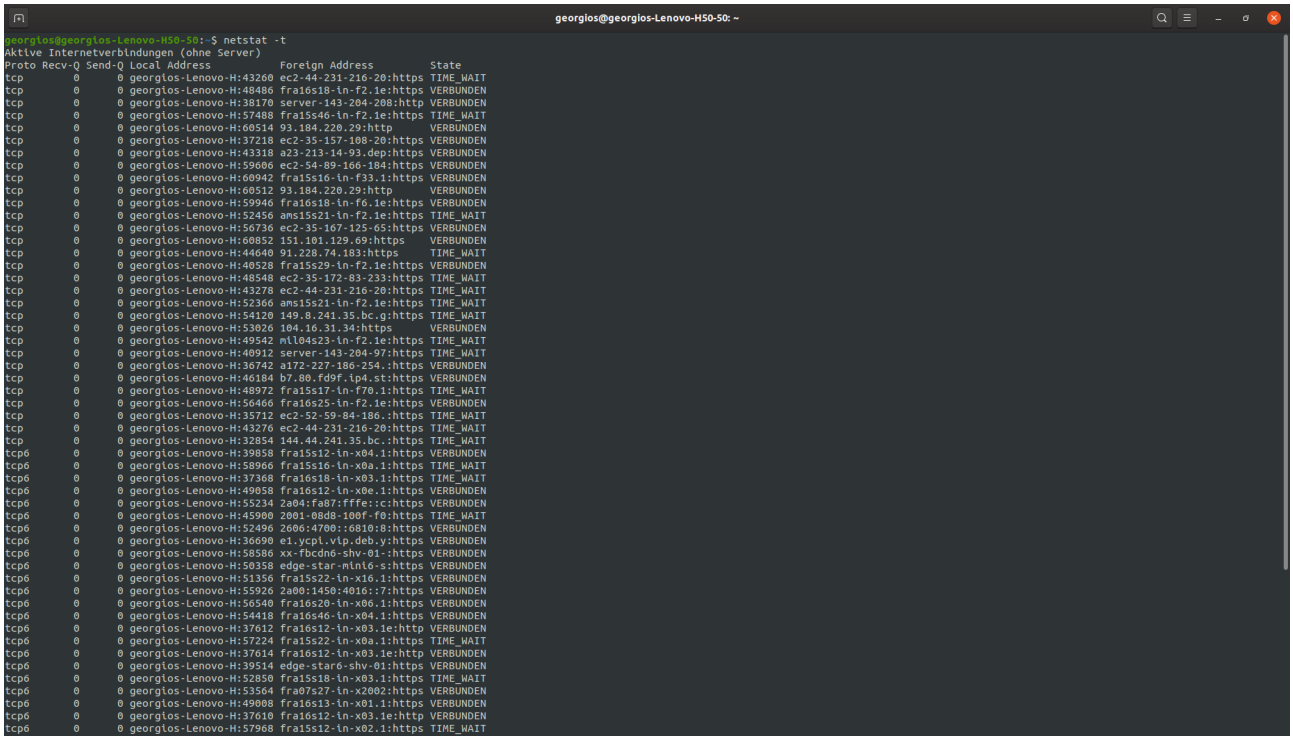
Übungsblatt 3

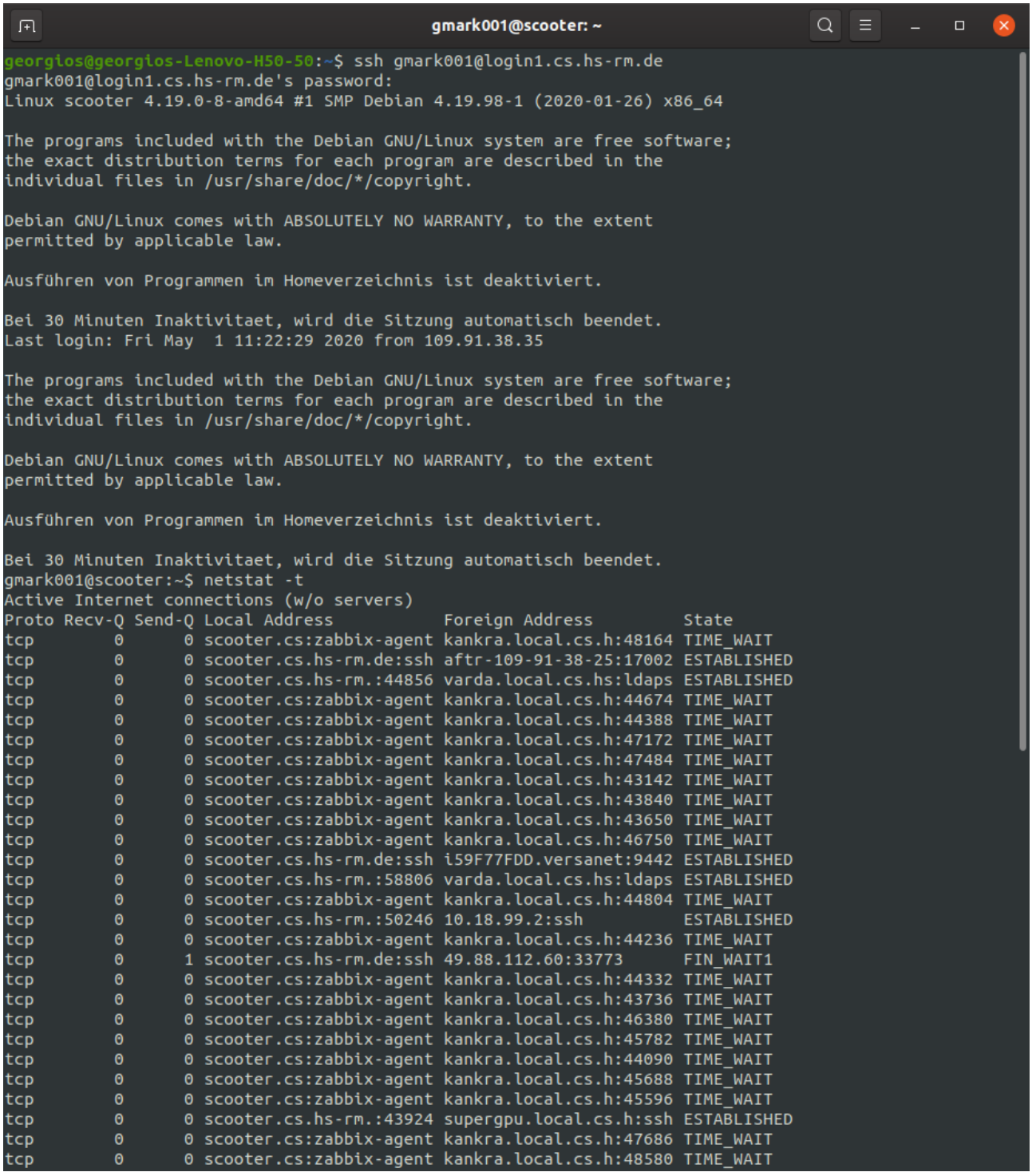
3.1)

a) Da netstat alle aktiven TCP-, UDP- und IP-Verbindungen und detaillierte TCP/IP-Daten anzeigen kann. Somit kann man fremde Verbindungen aufspüren.

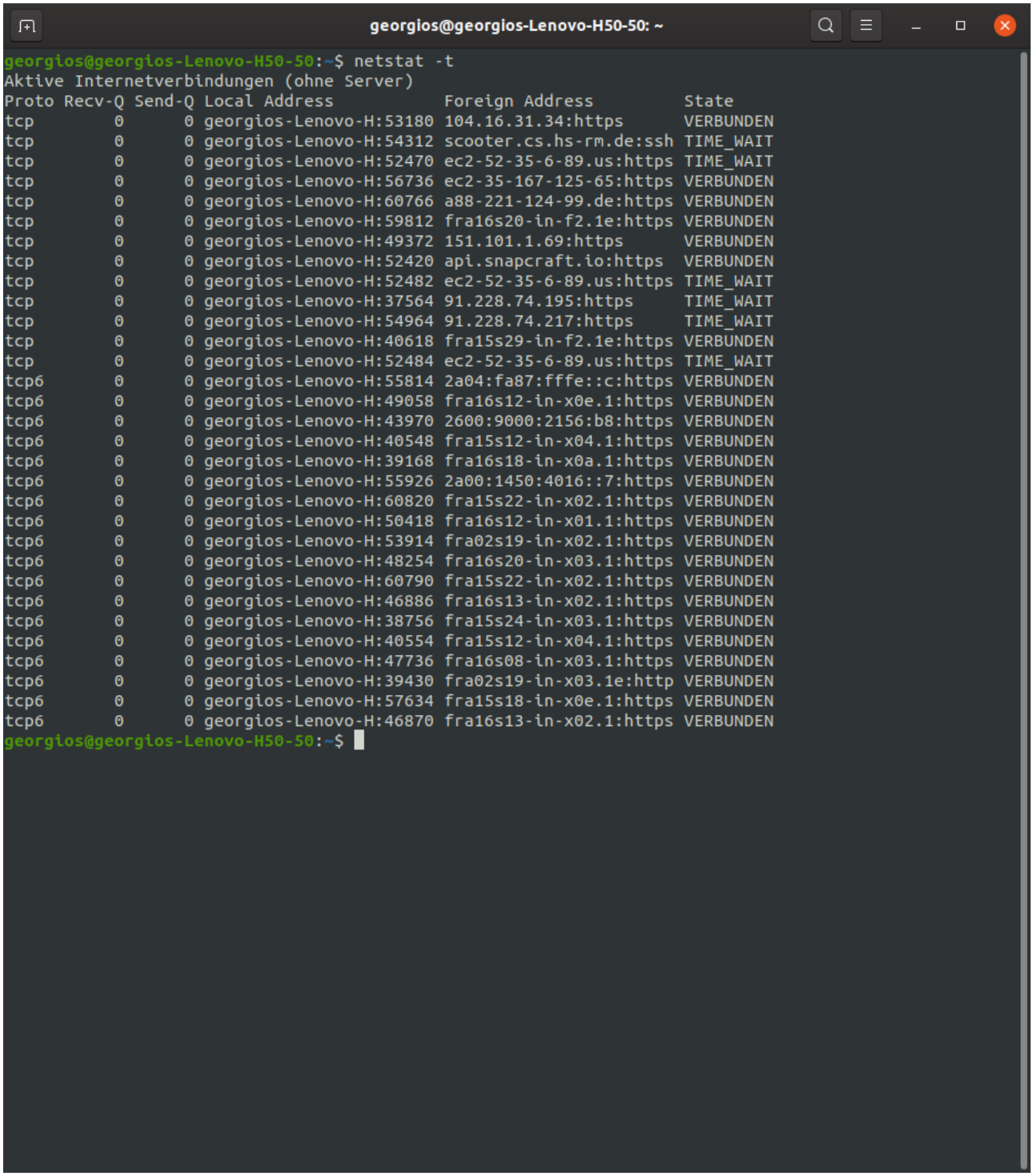
b) Mit „netstat -t“ sieht man alle aktive Verbindungen.



c)


gmark001@scooter: ~
georgios@georgios-Lenovo-H50-50:~$ ssh gmark001@login1.cs.hs-rm.de
gmark001@login1.cs.hs-rm.de's password:
Linux scooter 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Ausführen von Programmen im Homeverzeichnis ist deaktiviert.
Bei 30 Minuten Inaktivitaet, wird die Sitzung automatisch beendet.
Last login: Fri May 1 11:22:29 2020 from 109.91.38.35
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Ausführen von Programmen im Homeverzeichnis ist deaktiviert.
Bei 30 Minuten Inaktivitaet, wird die Sitzung automatisch beendet.
gmark001@scooter:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:48164 TIME_WAIT
tcp 0 0 scooter.cs.hs-rm.de:ssh aftr-109-91-38-25:17002 ESTABLISHED
tcp 0 0 scooter.cs.hs-rm.:44856 varda.local.cs.hs:ldaps ESTABLISHED
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:44674 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:44388 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:47172 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:47484 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:43142 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:43840 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:43650 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:46750 TIME_WAIT
tcp 0 0 scooter.cs.hs-rm.de:ssh i59F77FDD.versanet:9442 ESTABLISHED
tcp 0 0 scooter.cs.hs-rm.:58806 varda.local.cs.hs:ldaps ESTABLISHED
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:44804 TIME_WAIT
tcp 0 0 scooter.cs.hs-rm.:50246 10.18.99.2:ssh ESTABLISHED
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:44236 TIME_WAIT
tcp 0 1 scooter.cs.hs-rm.de:ssh 49.88.112.60:33773 FIN_WAIT1
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:44332 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:43736 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:46380 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:45782 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:44090 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:45688 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:45596 TIME_WAIT
tcp 0 0 scooter.cs.hs-rm.:43924 supergpu.local.cs.h:ssh ESTABLISHED
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:47686 TIME_WAIT
tcp 0 0 scooter.cs:zabbix-agent kankra.local.cs.h:48580 TIME_WAIT

d)


georgios@georgios-Lenovo-H50-50: ~
georgios@georgios-Lenovo-H50-50:~$ netstat -t
Aktive Internetverbindungen (ohne Server)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 georgios-Lenovo-H:53180 104.16.31.34:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:54312 scooter.cs.hs-rm.de:ssh TIME_WAIT
tcp 0 0 georgios-Lenovo-H:52470 ec2-52-35-6-89.us:https TIME_WAIT
tcp 0 0 georgios-Lenovo-H:56736 ec2-35-167-125-65:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:60766 a88-221-124-99.de:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:59812 fra16s20-in-f2.1e:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:49372 151.101.1.69:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:52420 api.snapcraft.io:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:52482 ec2-52-35-6-89.us:https TIME_WAIT
tcp 0 0 georgios-Lenovo-H:37564 91.228.74.195:https TIME_WAIT
tcp 0 0 georgios-Lenovo-H:54964 91.228.74.217:https TIME_WAIT
tcp 0 0 georgios-Lenovo-H:40618 fra15s29-in-f2.1e:https VERBUNDEN
tcp 0 0 georgios-Lenovo-H:52484 ec2-52-35-6-89.us:https TIME_WAIT
tcp6 0 0 georgios-Lenovo-H:55814 2a04:fa87:fffe::c:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:49058 fra16s12-in-x0e.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:43970 2600:9000:2156:b8:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:40548 fra15s12-in-x04.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:39168 fra16s18-in-x0a.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:55926 2a00:1450:4016::7:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:60820 fra15s22-in-x02.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:50418 fra16s12-in-x01.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:53914 fra02s19-in-x02.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:48254 fra16s20-in-x03.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:60790 fra15s22-in-x02.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:46886 fra16s13-in-x02.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:38756 fra15s24-in-x03.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:40554 fra15s12-in-x04.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:47736 fra16s08-in-x03.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:39430 fra02s19-in-x03.1e:http VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:57634 fra15s18-in-x0e.1:https VERBUNDEN
tcp6 0 0 georgios-Lenovo-H:46870 fra16s13-in-x02.1:https VERBUNDEN
georgios@georgios-Lenovo-H50-50:~$

3.2)

a) Mithilfe von Wireshark kann man Pakete von vielen Protokollen analysieren. Das verstößt gegen die Privatsphäre der Personen die das eigene Internet verwenden. Es kann jedoch legal verwendet werden um eine bestehende Internetverbindung zu überprüfen z.B auf fremde Benutzer

e) Man kann auswählen welche Pakete man mitloggen möchte z.B TCP Protokoll, Zielport Quelladresse.

f) Die ersten 4 Bits(0100) vom erstem Byte(0x45) stehen für die Version (4), die restlichen 4 Bits (0101) stehen für die Headerlänge(5 * 32 Bytes). Das nächste Byte(0x0) beschreibt den Type of Service. Die ersten 3 Bits beschreiben die Priorität und die nächsten 4 Bits beschreiben jeweils lowdelay, throughput, reliability, lowcost und das letzte Byte muss 0 sein. In dem Fall ist keins der Flags gesetzt. Die nächsten 2 Bytes(0x005C) geben die Header- und Datenlänge an, in dem Fall 92 Bytes. Die nächsten 2 Bytes(0x4D1E) sind die Identification, in dem Fall ist die Kennnummer vom Sender 19742. Das nächste Bit(0) wird nicht verwendet(ist reserviert). Das nächste Bit(0) ist das Don‘t Fragment Bit, d.h. dass das paket nicht in kleinere Pakete aufgeteilt werden darf. Das nächste Bit ist das More Fragments Bit, gibt an ob das Paket fragmentiert wurde und ein Teil-Paket folgt. Die nächsten 13 Bits(0) sind der Fragment Offset in 8 Byte Einheiten und geben den Offset an dem die Datensektion anfängt. Das nächste Byte(0x3D) gibt die TTL an, in dem Fall 61 Sekunden. Das nächste Byte(0x01) gibt das Transportprotoll an, hier ICMP. Die nächste 2 Bytes(0xF4CD) sind die Header Checksumme. Die nächste 4 Bytes(0xC3486689) sind die Quelle, hier „195.72.102.137“. Die nächste 4 Bytes(0x0A9C0748) sind das Ziel, hier „10.156.7.72“ .

g) 1)

von rechts nach links: Nummer des Paketes, Quelle, Ziel

No.	Source	Destination	Time
1	10.156.7.72	195.72.102.137	0.000000
2	10.156.7.254	10.156.7.72	0.001213
3	10.156.7.72	195.72.102.137	0.002379
4	10.156.7.254	10.156.7.72	0.003476
5	10.156.7.72	195.72.102.137	0.004630
6	10.156.7.254	10.156.7.72	0.005828
7	10.156.7.72	195.72.102.137	5.560819
8	195.72.102.209	10.156.7.72	5.562608
9	10.156.7.72	195.72.102.137	5.621381
10	195.72.102.209	10.156.7.72	5.622911
11	10.156.7.72	195.72.102.137	5.687440
12	195.72.102.209	10.156.7.72	5.689514
13	10.156.7.72	195.72.102.137	6.690293
14	195.72.102.204	10.156.7.72	6.692242
15	10.156.7.72	195.72.102.137	6.693953
16	195.72.102.204	10.156.7.72	6.695628
17	10.156.7.72	195.72.102.137	6.697119
18	195.72.102.204	10.156.7.72	6.698785
19	10.156.7.72	195.72.102.137	7.703877
20	195.72.102.137	10.156.7.72	7.705838
21	10.156.7.72	195.72.102.137	7.707312
22	195.72.102.137	10.156.7.72	7.709104
23	10.156.7.72	195.72.102.137	7.710576
24	195.72.102.137	10.156.7.72	7.712425

2) es wird überall das Protokoll ICMP verwendet

3) diese Pakete haben TTL 0 erreicht und werden nicht weitergeleitet

4)

1, 3, 5 ICMP ECHO REQUEST an 195.72.102.137 mit TTL 1 (3xwiederholt)

2, 4, 6 ICMP TTL EXCEEDED von 10.156.7.254 (1. Router)

7, 9, 11 ICMP ECHO REQUEST an 195.72.102.137 mit TTL 2 (3xwiederholt)

8, 10, 12 ICMP TTL EXCEEDED von 195.72.102.209

13, 15, 17 ICMP ECHO REQUEST an 195.72.102.137 mit TTL 3 (3xwiederholt)

14, 16, 18 ICMP TTL EXCEEDED von 195.72.102.204

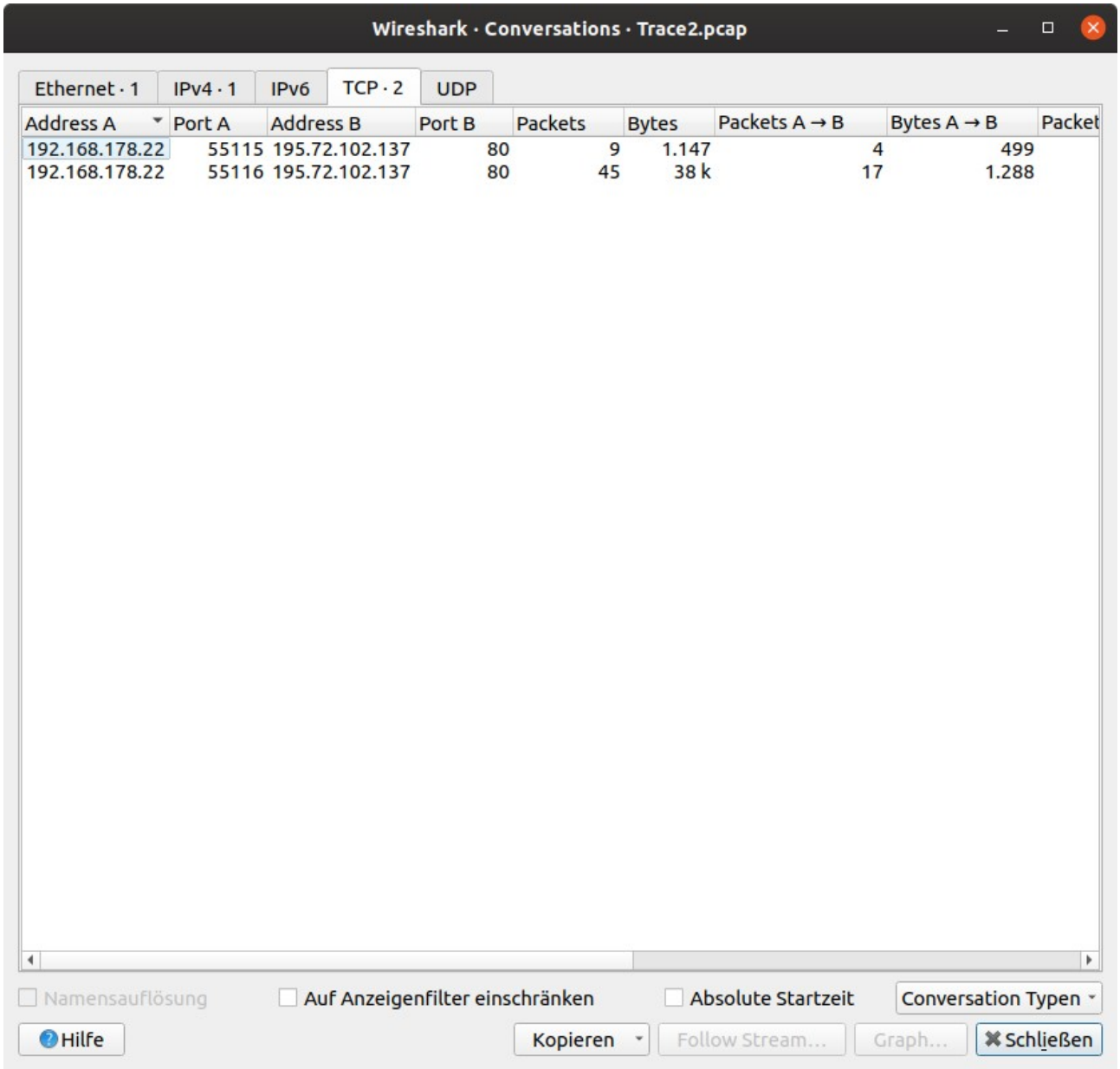
19, 21, 23 ICMP ECHO REQUEST an 195.72.102.137 mit TTL 4 (3xwiederholt)

20, 22, 24 ICMP ECHO Reply an 195.72.102.137 mit TTL 61 (3xwiederholt)

5) Bei allen rosa Paketen mit source=10.156.7.72 wurde der Befehl „ping 195.72.102.137“ ausgeführt. Bei allen anderen Paketen wurde auf diesen Befehl geantwortet siehe Aufgabe 4.

3.3)

a) 1) Es sind insgesamt 2 TCP-Verbindungen



2, 3) Beispiel Paket 15:

```
$OwE"O*°¿EÖ¹X@5ê:AHfÁ¨²P×L'~b¼-èP{(HTTP/1.1 200 OK
Date: Mon, 10 Nov 2014 08:40:35 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.23
Set-Cookie: fe_typo_user=71ff7d48acfd5ab1b3f5d48b63aefcc4; path=/; httponly
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

8bac
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html
     PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xml:lang="de-DE" lang="de-DE" xmlns="http://www.w3.org/1999/xhtml">
<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<!--
        This website is powered by TYPO3 - inspiring people to share!
        TYPO3 is a free open source Content Management Framework initially created by Kasper Skaarhoj and licensed under GNU/GPL.
        TYPO3 is copyright 1998-2013 of Kasper Skaarhoj. Extensions are copyright of their respective owners.
        Information and contribution at http://typo3.org/
-->

<base href="http://www.hs-rm.de/" />
<link rel="shortcut icon" href="http://www.hs-rm.de/typo3conf/ext/hsrm_template/resource/public/img/favicon.ico" type="image/png; charset=binary" />
<link rel="icon" href="http://www.hs-rm.de/typo3conf/ext/hsrm_template/resource/public/img/favicon.ico" type="image/png; charset=binary" />
<title>Hochschule RheinMain</title>
<meta name="generator" content="TYPO3 6.1 CMS" />
<meta name="description" content="Startseite der Hochschule" />
<meta name="keywor
```

b) 1) Diese drei Pakete haben die Funktion eine Verbindung zwischen Client und Server zu ermöglichen. Das SYN-Paket (vom Client) dient dazu die Verbindung zu starten und die SEQ-Werte zu synchronisieren. Als nächstes sendet der Server das SYN/ACK-Paket als Bestätigung und der Client sendet ein ACK-Paket als Bestätigung an den Server.

2) Als Beispiel habe ich Paket 10(ACK), 11(SYN/ACK) und 12(ACK) ausgewählt.
SEQ = 1; ACK = 1

3) Es wurden 24 Segmente von 195.72.102.137 übertragen. Alle Segmente haben Len=1452.

15	195.72.102.137	192.168.178.22	0.352141	TCP	1506	80 → 55116 [ACK] Seq=1 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
16	195.72.102.137	192.168.178.22	*REF*	TCP	1506	80 → 55116 [ACK] Seq=1453 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
18	195.72.102.137	192.168.178.22	0.000415	TCP	1506	80 → 55116 [ACK] Seq=2905 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
19	195.72.102.137	192.168.178.22	0.000995	TCP	1506	80 → 55116 [ACK] Seq=4357 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
21	195.72.102.137	192.168.178.22	0.001426	TCP	1506	80 → 55116 [ACK] Seq=5809 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
22	195.72.102.137	192.168.178.22	0.001768	TCP	1506	80 → 55116 [ACK] Seq=7261 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
24	195.72.102.137	192.168.178.22	0.002151	TCP	1506	80 → 55116 [ACK] Seq=8713 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
25	195.72.102.137	192.168.178.22	0.002897	TCP	1506	80 → 55116 [PSH, ACK] Seq=10165 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
27	195.72.102.137	192.168.178.22	0.003157	TCP	1506	80 → 55116 [ACK] Seq=11617 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
28	195.72.102.137	192.168.178.22	0.003782	TCP	1506	80 → 55116 [ACK] Seq=13069 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
30	195.72.102.137	192.168.178.22	0.015621	TCP	1506	80 → 55116 [ACK] Seq=14521 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
31	195.72.102.137	192.168.178.22	0.017977	TCP	1506	80 → 55116 [PSH, ACK] Seq=15973 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
33	195.72.102.137	192.168.178.22	0.021068	TCP	1506	80 → 55116 [ACK] Seq=17425 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
34	195.72.102.137	192.168.178.22	0.022447	TCP	1506	80 → 55116 [ACK] Seq=18877 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
36	195.72.102.137	192.168.178.22	0.025738	TCP	1506	80 → 55116 [ACK] Seq=20329 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
37	195.72.102.137	192.168.178.22	0.027340	TCP	1506	80 → 55116 [ACK] Seq=21781 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
39	195.72.102.137	192.168.178.22	0.032624	TCP	1506	80 → 55116 [ACK] Seq=23233 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
40	195.72.102.137	192.168.178.22	0.033187	TCP	1506	80 → 55116 [ACK] Seq=24685 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
42	195.72.102.137	192.168.178.22	0.035658	TCP	1506	80 → 55116 [ACK] Seq=26137 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
43	195.72.102.137	192.168.178.22	0.037060	TCP	1506	80 → 55116 [PSH, ACK] Seq=27589 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
45	195.72.102.137	192.168.178.22	0.040205	TCP	1506	80 → 55116 [ACK] Seq=29041 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
46	195.72.102.137	192.168.178.22	0.042027	TCP	1506	80 → 55116 [ACK] Seq=30493 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
48	195.72.102.137	192.168.178.22	0.044094	TCP	1506	80 → 55116 [ACK] Seq=31945 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]
50	195.72.102.137	192.168.178.22	0.046562	TCP	1506	80 → 55116 [ACK] Seq=33397 Ack=359 Win=15744 Len=1452 [TCP segment of a reassembled PDU]

4) 66 + 412 + 15 * 64 = 1438 Bytes (Len = 0, es geht in dem Fall nur um die Header)

10	192.168.178.22	195.72.102.137	0.166542	TCP	66
12	192.168.178.22	195.72.102.137	0.188281	TCP	54
13	192.168.178.22	195.72.102.137	0.188604	HTTP	412
17	192.168.178.22	195.72.102.137	0.000093	TCP	54
20	192.168.178.22	195.72.102.137	0.001061	TCP	54
23	192.168.178.22	195.72.102.137	0.001829	TCP	54
26	192.168.178.22	195.72.102.137	0.002959	TCP	54
29	192.168.178.22	195.72.102.137	0.003833	TCP	54
32	192.168.178.22	195.72.102.137	0.018067	TCP	54
35	192.168.178.22	195.72.102.137	0.022509	TCP	54
38	192.168.178.22	195.72.102.137	0.027459	TCP	54
41	192.168.178.22	195.72.102.137	0.033264	TCP	54
44	192.168.178.22	195.72.102.137	0.037162	TCP	54
47	192.168.178.22	195.72.102.137	0.042131	TCP	54
49	192.168.178.22	195.72.102.137	0.045683	TCP	54
52	192.168.178.22	195.72.102.137	0.049226	TCP	54
53	192.168.178.22	195.72.102.137	0.049475	TCP	54

5) Paket 9: Win=8192

Paket 10: Win=14600

Paket 11: Win=17424

10	192.168.178.22	195.72.102.137	0.166542	TCP	66	55116 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
11	195.72.102.137	192.168.178.22	0.188137	TCP	66	80 → 55116 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=128
12	192.168.178.22	195.72.102.137	0.188281	TCP	54	55116 → 80 [ACK] Seq=1 Ack=1 Win=17424 Len=0