R|R|Z|N

Leibniz Universität Hannover

Mac Firewall etc.

Mark Heisterkamp

heisterkamp@rrzn.uni-hannover.de

10. August 2009

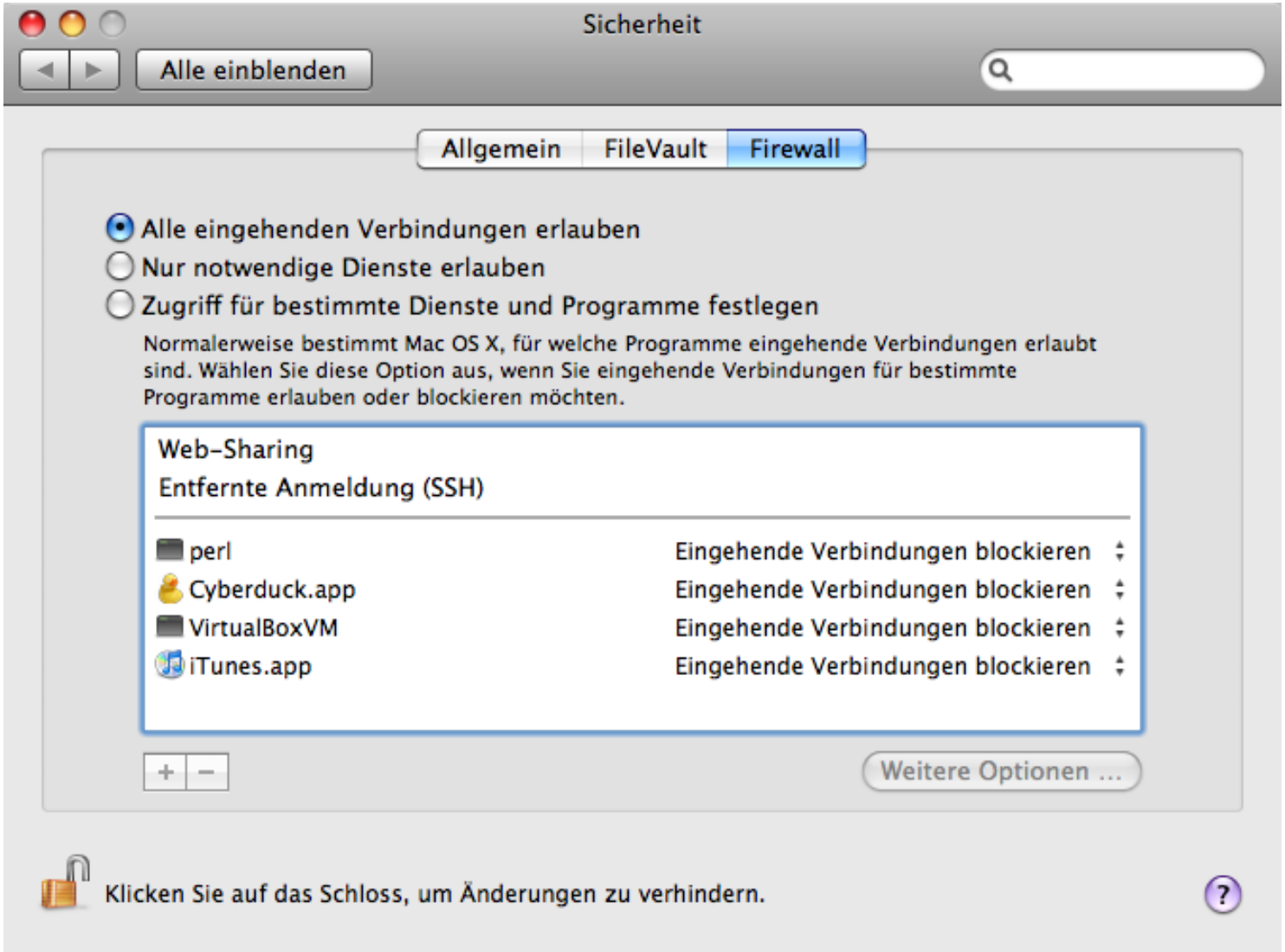
Leopard

Seit Mac OS X 10.5 zwei Firewalls:

- Applikationsspezifisch
- ipfw (Free-BSD)

Wobei ipfw maßgeblich ist. Jede ipfw-Beschränkung gilt unabhängig von der Applikations-Firewall.

Applikationsspezifisch

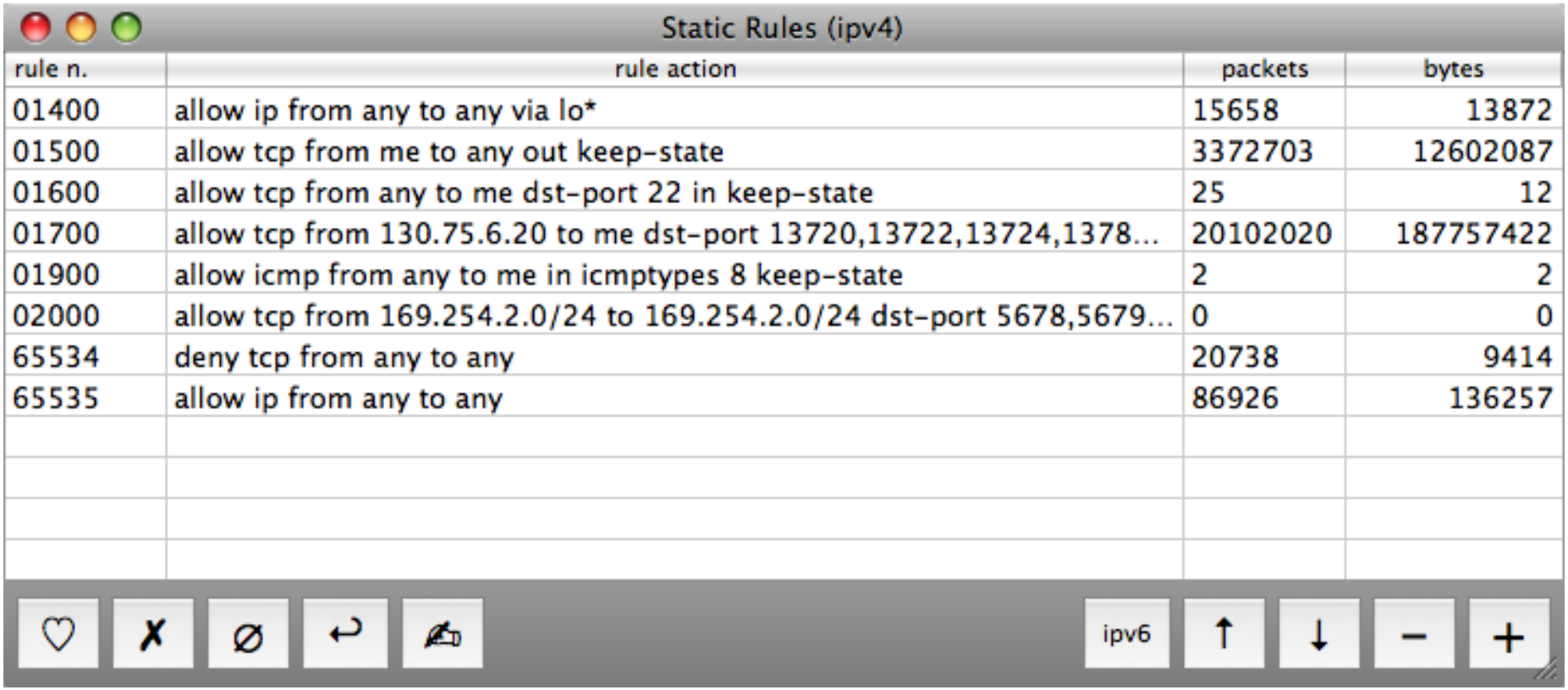


ipfw

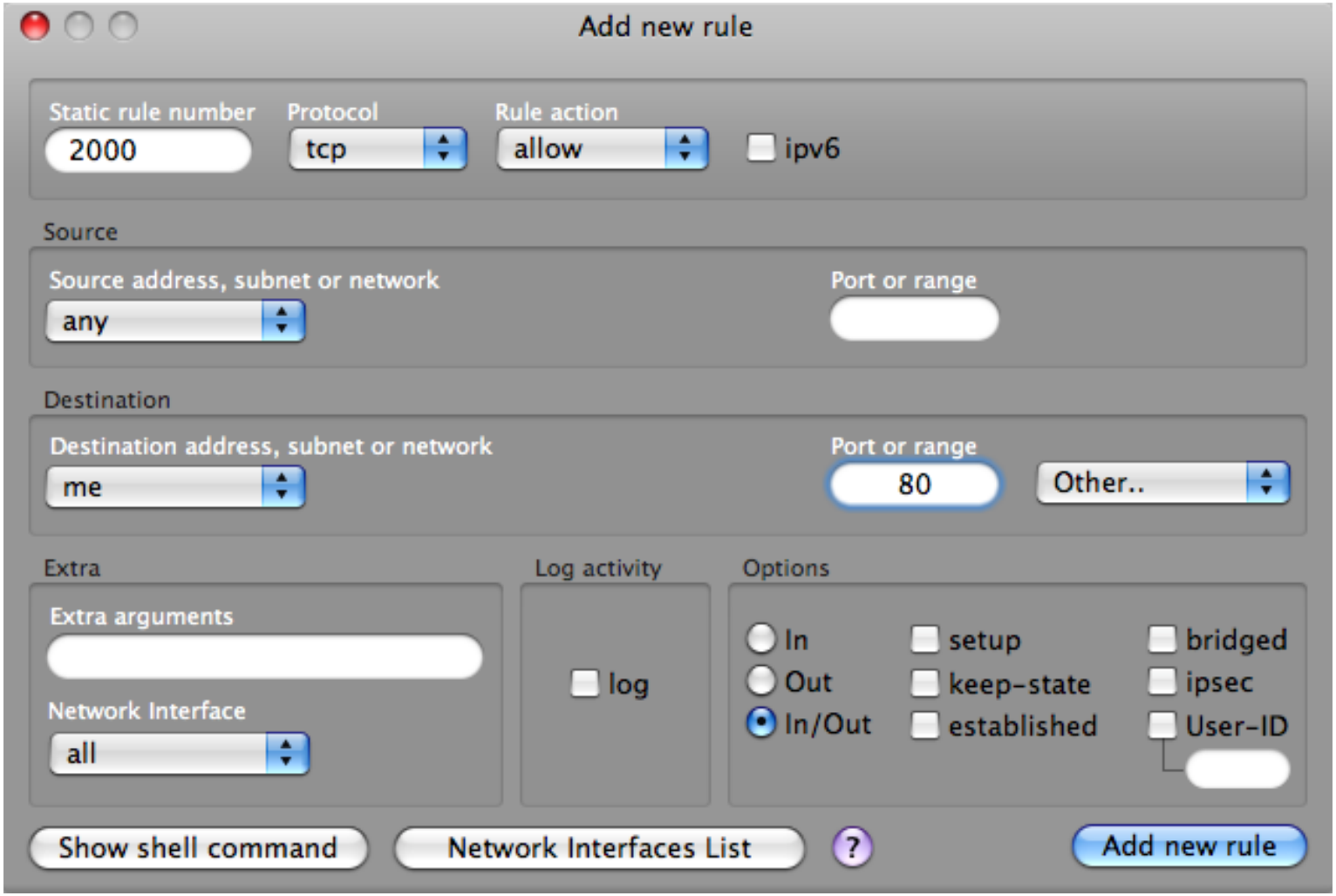
```
sudo ipfw disable firewall
```

```
mheiste@IntelKawumm:~>sudo ipfw list
01400 allow ip from any to any via lo*
01500 allow tcp from me to any out keep-state
01600 allow tcp from any to me dst-port 22 in keep-state
01700 allow tcp from 130.75.6.20 to me dst-port \
13720,13722,13724,13782,13783 in keep-state
01900 allow icmp from any to me in icmptypes 8 keep-state
65534 deny tcp from any to any
65535 allow ip from any to any
```

WaterRoof (ipfw-Frontend)



Port 80 – WaterRoof



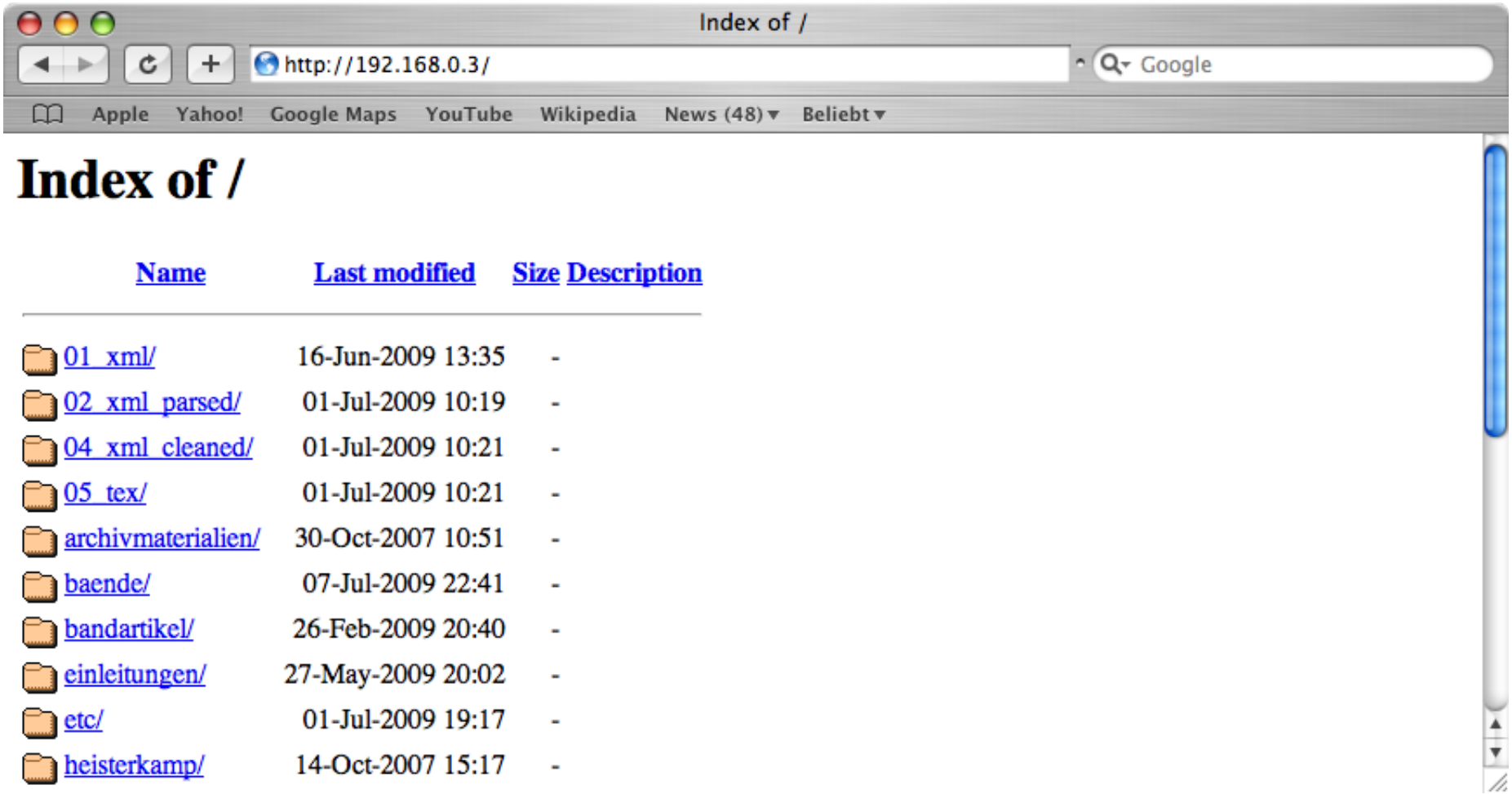
Port 80 – WaterRoof (Ergebnis)

Static Rules (ipv4)

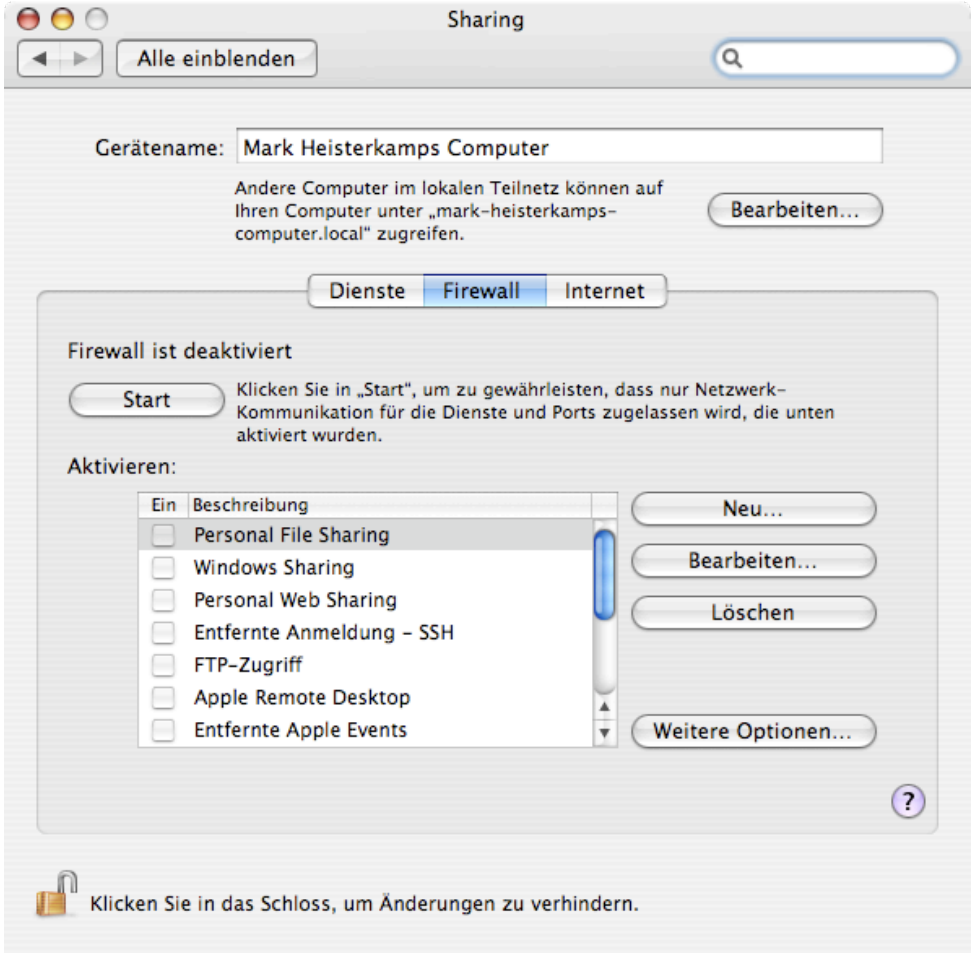
rule n.	rule action	packets	bytes
00800	allow ip from any to any via lo*	12	9
01400	allow tcp from me to any out keep-state	571	1209
01500	allow tcp from any to me dst-port 22 in keep-state	0	0
01600	allow tcp from 130.75.6.20 to me dst-port 13720,13722,13724,1378...	0	0
01700	allow icmp from any to me in icmptypes 8 keep-state	0	0
01900	allow tcp from 169.254.2.0/24 to 169.254.2.0/24 dst-port 5678,5679...	0	0
02000	allow tcp from any to me dst-port 80	0	0
65534	deny tcp from any to any	20	10
65535	allow ip from any to any	87269	136564

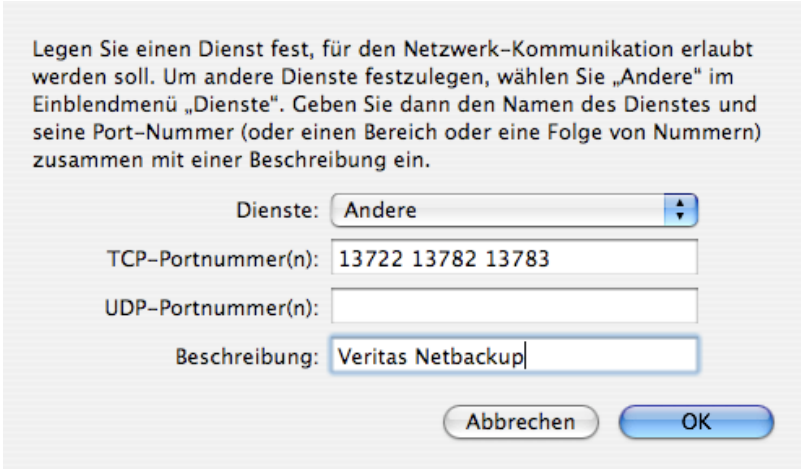
♡ ✗ ⌀ ↩ ✍ ipv6 ↑ ↓ − +

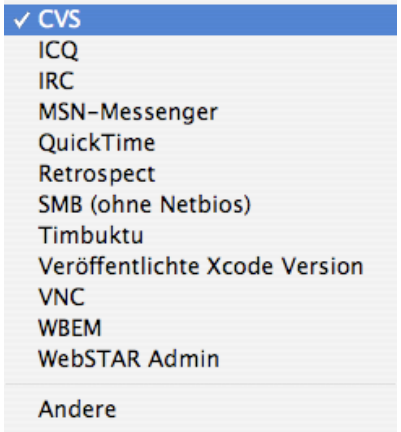
Port 80 – Safari



10.4 (Tiger) ipfw-Frontend



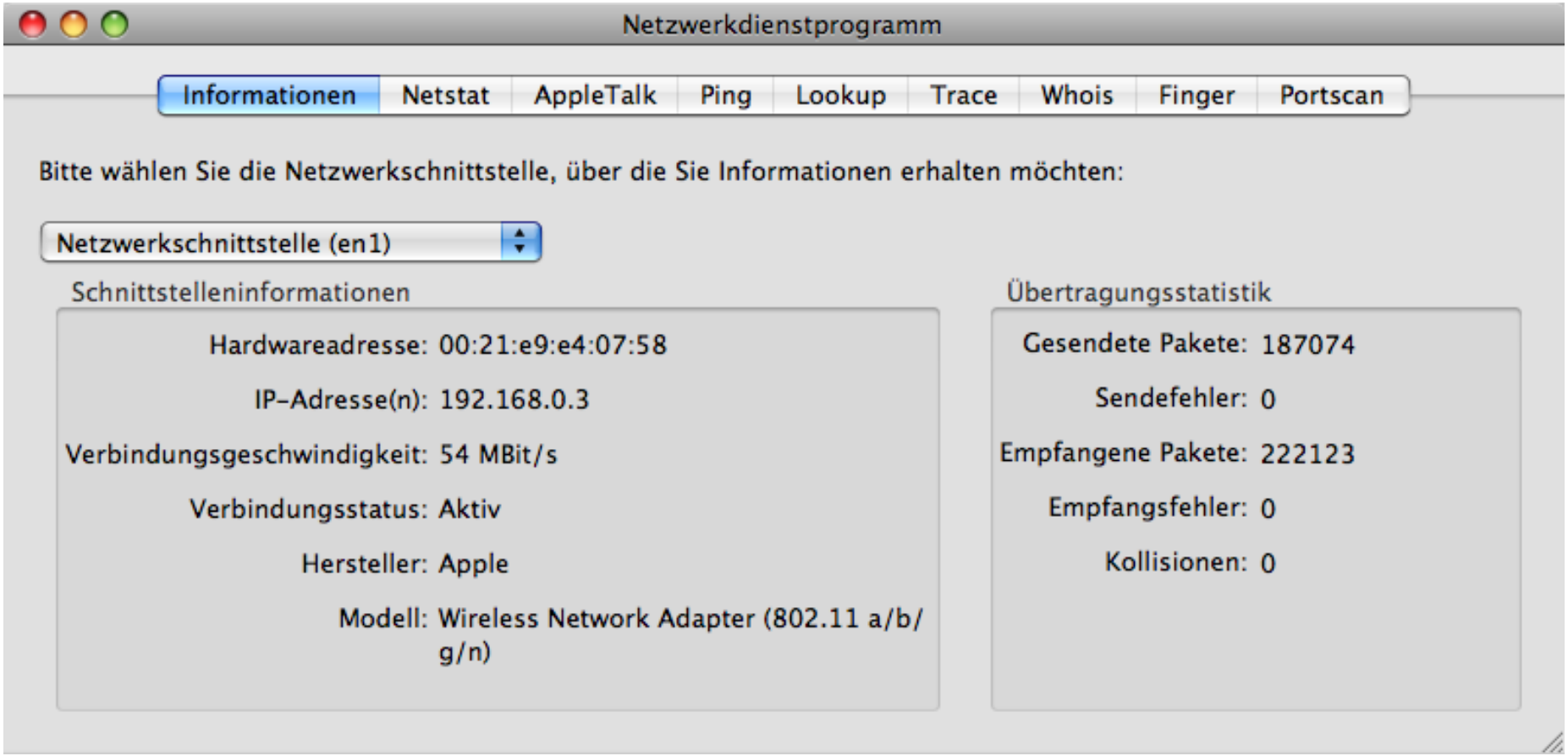




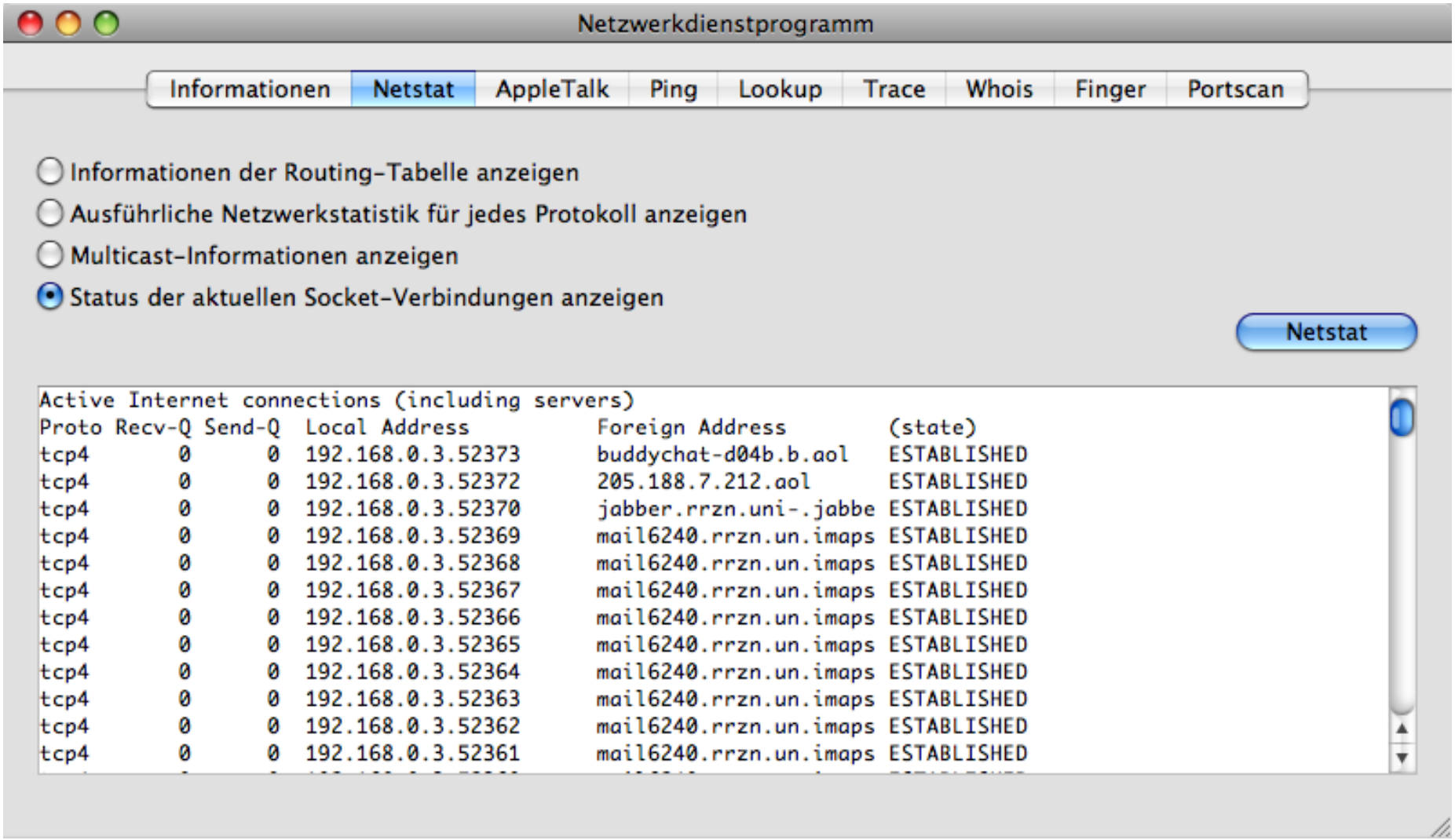
Tools – Frontend

- Netzwerkdienstprogramm
- Sophos
  http://www.rrzn.uni-hannover.de/antiviren.html
- iStat menus
  http://www.islayer.com/apps/istatmenus/

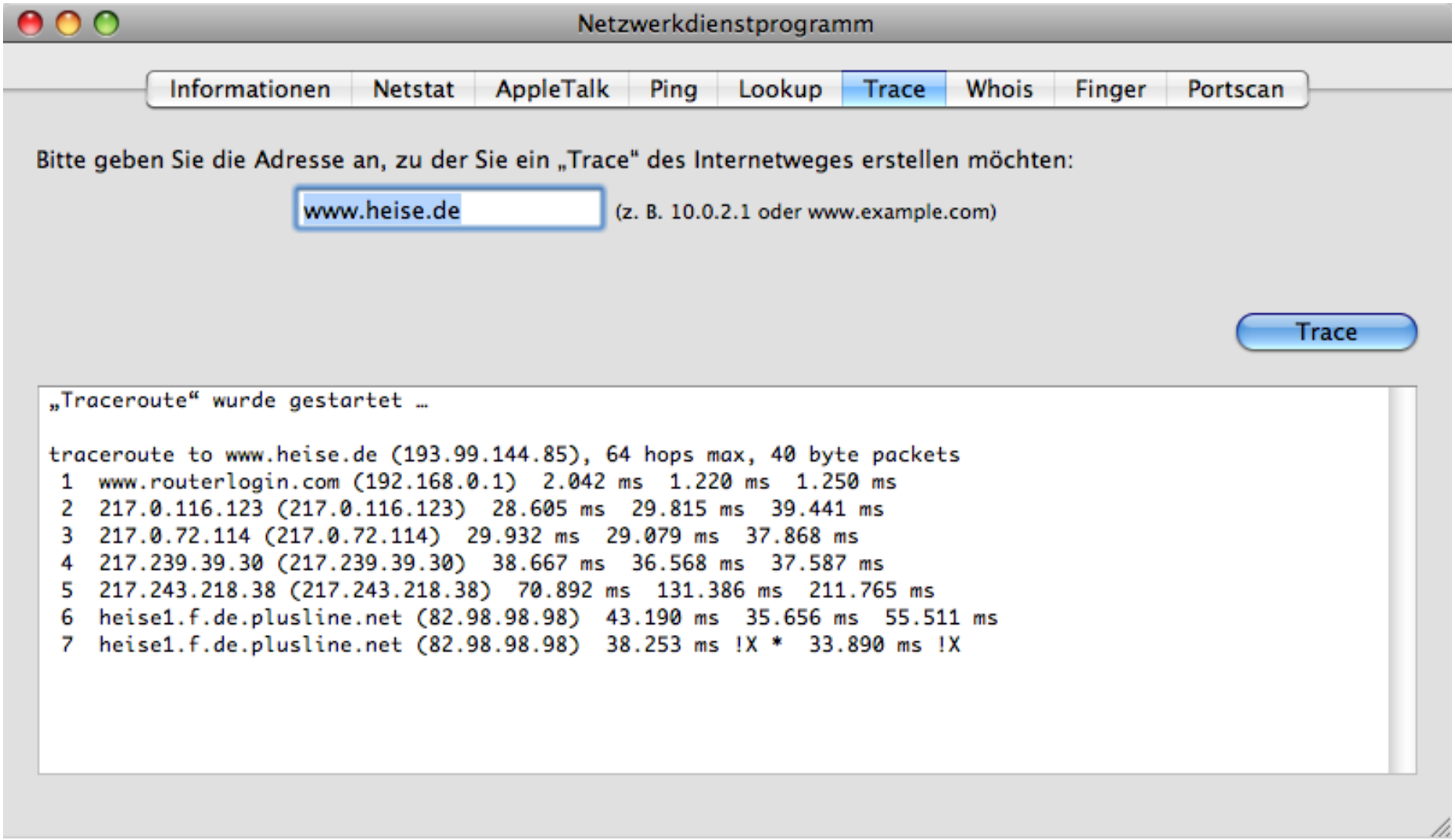
Netzwerkdienstprogramm



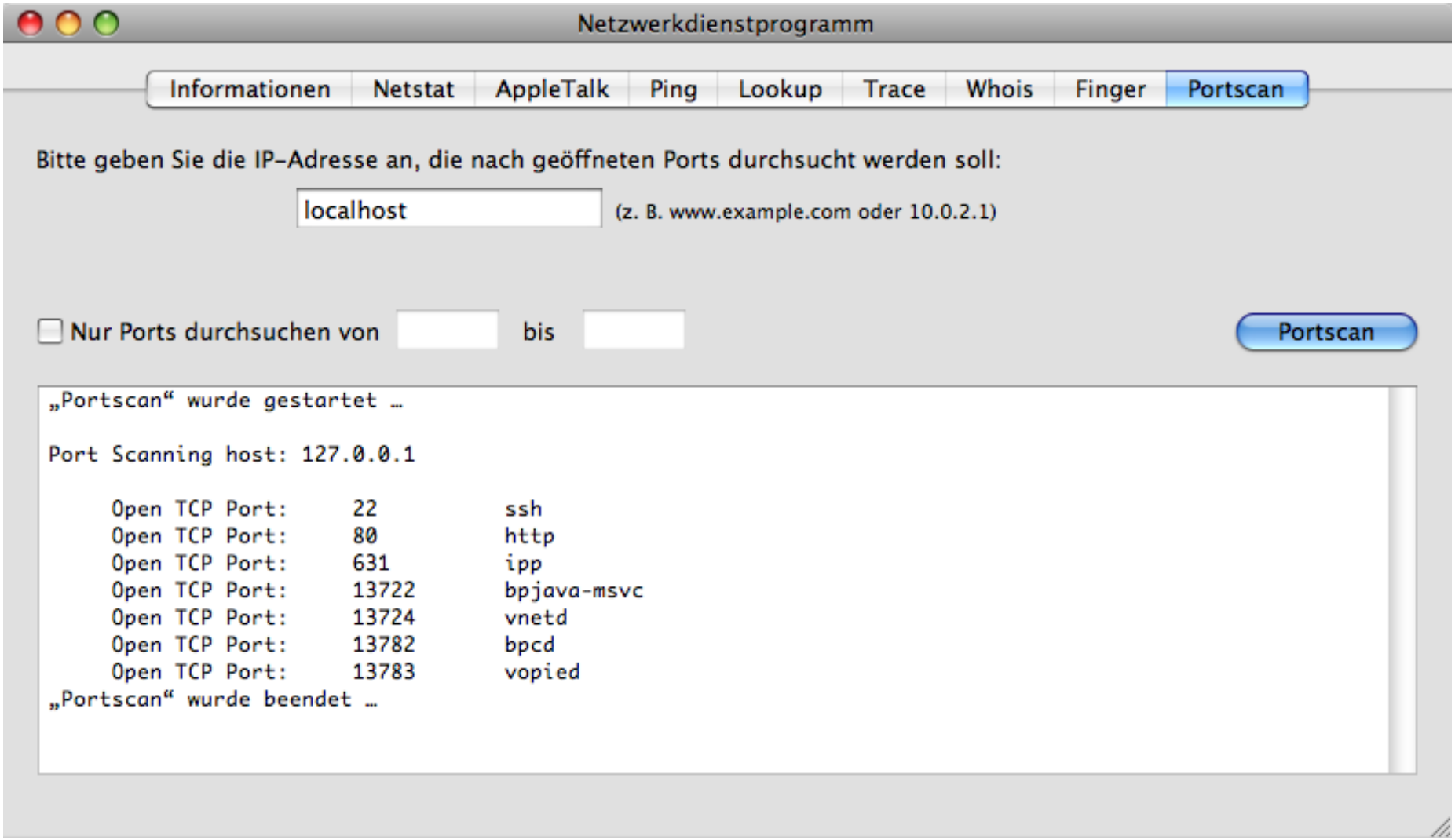
Netzwerkdienstprogramm – netstat



Netzwerkdienstprogramm – traceroute



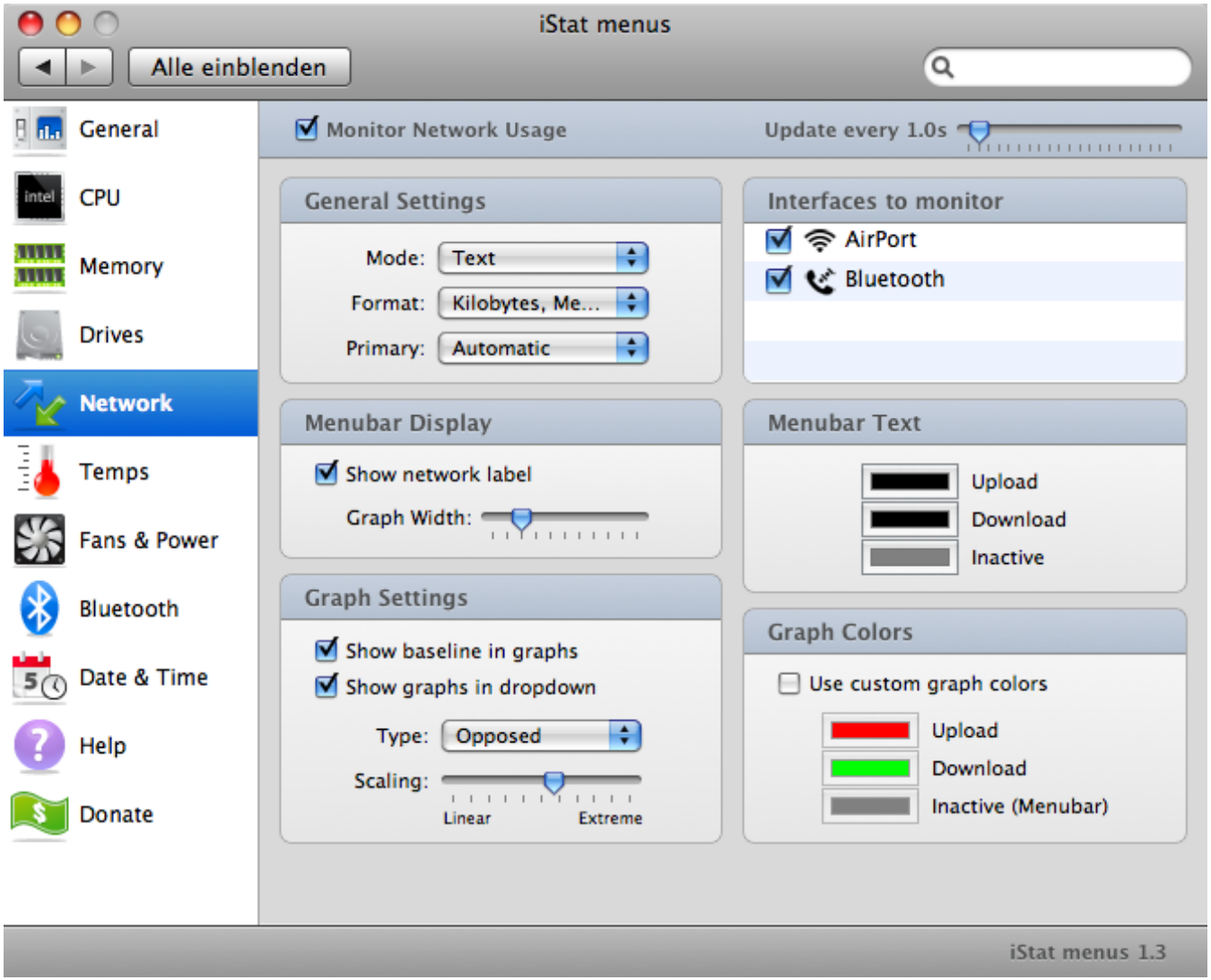
Netzwerkdienstprogramm – portscan



Sophos

- z.Zt. 30 Viren in der Sophos-online-Datenbank
- unauffällig, praktisch

iStat menus


iStat menus
Alle einblenden
General
CPU
Memory
Drives
Network
Temps
Fans & Power
Bluetooth
Date & Time
Help
Donate
Monitor Network Usage
Update every 1.0s
General Settings
Mode: Text
Format: Kilobytes, Me...
Primary: Automatic
Interfaces to monitor
AirPort
Bluetooth
Menubar Display
Show network label
Graph Width:
Menubar Text
Upload
Download
Inactive
Graph Settings
Show baseline in graphs
Show graphs in dropdown
Type: Opposed
Scaling:
Linear
Extreme
Graph Colors
Use custom graph colors
Upload
Download
Inactive (Menubar)
iStat menus 1.3

Tools – Kommandozeile

System-Tools:

- lsof
- netstat
- tcpdump

Zusatz-Tools

- fink http://www.finkproject.org
  - nmap
  - iftop

Nach Hause telefonieren ...

```
lsof -i +c0 -r
```

`-i` Netzwerk-Dateien anzeigen (evtl. mit IP, Hostname, Protokolltyp etc.)

`+c0` Kommandonamen ausschreiben

`-r` Repeat-Mode (Endlosschleife)

netstat

Mac OS X setzt netstat in einer recht alten BSD-Variante ein, deren Kommandozeilenparameter sich wesentlich von der GNU-Version unterscheiden.

Insbesondere funktioniert folgendes nicht:

```
netstat -apW -inet -numeric-ports
```

`-p` PID und Kommandoname

`-W` Wide, nix wird abgeschnitten im Terminal

`--numeric-ports` Ports als Nummern

Schöne netstat-Ausgabe (GNU)

```
heisterkamp@webdav:~$ sudo netstat -apW --inet --numeric-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      22069/slapd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      278/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      561/exim4
tcp        0      0 127.0.0.1:389           127.0.0.1:38963         ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389           127.0.0.1:41420         ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389           127.0.0.1:39612         ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:49711         127.0.0.1:389           ESTABLISHED 28977/apache2
tcp        0      0 127.0.0.1:48855         127.0.0.1:389           ESTABLISHED 5386/apache2
tcp        0      0 127.0.0.1:389           127.0.0.1:48855         ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389           127.0.0.1:43458         ESTABLISHED 22069/slapd
tcp        0      0 130.75.6.15:22          130.75.6.189:57483      ESTABLISHED 15517/sshd: heister
tcp        0      0 127.0.0.1:48857         127.0.0.1:389           ESTABLISHED 28979/apache2
tcp        0      0 127.0.0.1:389           127.0.0.1:39626         ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:43458         127.0.0.1:389           ESTABLISHED 5383/apache2
tcp        0      0 127.0.0.1:39612         127.0.0.1:389           ESTABLISHED 28975/apache2
tcp        0      0 127.0.0.1:38963         127.0.0.1:389           ESTABLISHED 5384/apache2
tcp        0      0 127.0.0.1:39626         127.0.0.1:389           ESTABLISHED 5382/apache2
tcp        0      0 127.0.0.1:41420         127.0.0.1:389           ESTABLISHED 28978/apache2
tcp        0      0 127.0.0.1:389           127.0.0.1:48857         ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389           127.0.0.1:49711         ESTABLISHED 22069/slapd
```

Nicht so schöne Mac-Ausgabe von netstat

```
mheiste@IntelKawumm:~>sudo netstat -a -f inet
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  192.168.0.3.62940      zen.rrzn.uni-han.ssh   ESTABLISHED
tcp4       0      0  192.168.0.3.62938      buddychat-d04b.b.aol   ESTABLISHED
tcp4       0      0  192.168.0.3.62937      205.188.7.212.aol      ESTABLISHED
tcp4       0      0  192.168.0.3.62935      jabber.rrzn.uni-.jabbe ESTABLISHED
tcp4       0      0  192.168.0.3.52369      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52368      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52367      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52366      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52365      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52364      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52363      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52362      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52361      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52360      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52359      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52358      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52357      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52356      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52355      mail6240.rrzn.un.imaps ESTABLISHED
tcp4       0      0  192.168.0.3.52354      mail6240.rrzn.un.imaps ESTABLISHED
```

tcpdump

```
sudo tcpdump -i en1 -qt ip
```

`-i en1` Interface 1 (Airport)

`-q` Quick output – kürzere Zeilen

`-t` Ohne Zeitstempel in jeder Zeile

`ip` Protokolltyp

tcpdump-Ausgabe

```
mheiste@IntelKawumm:~>sudo tcpdump -i en1 -qt ip
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 0
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP 192.168.0.3.63031 > www.heise.de.http: tcp 419
IP www.heise.de.http > 192.168.0.3.63031: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP www.heise.de.http > 192.168.0.3.63031: tcp 8
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP 192.168.0.3.63032 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP 192.168.0.3.63033 > www.heise.de.http: tcp 0
```

nmap

```
mheiste@IntelKawumm:~>nmap -P0 localhost

Starting Nmap 4.20 ( http://insecure.org ) at 2009-08-09 22:44 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1336 closed ports, 355 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
13722/tcp open  VeritasNetbackup
13782/tcp open  VeritasNetbackup
13783/tcp open  VeritasNetbackup

Nmap finished: 1 IP address (1 host up) scanned in 9.339 seconds
```

sudo iftop –i en1