

Der Werkzeugkasten

Kommunales Rechenzentrum Niederrhein (KRZN)
Friedrich-Heinrich-Allee 130
47475 Kamp-Lintfort
Internet: www.krzn.de

Vortrag: Charly Kühnast

Alle möglichen und
unmöglichen, bekannten
und unbekannten Tools
für den Linux-Admin



TCPFlow: Wireshark für Arme

Sniffer, der Verbindungen zu „Flows“ zusammenfasst und menschenlesbar präsentiert.

`tcpflow -i eth0 -c -e port 80`

-c: auf Konsole

-e: bunt

Beispiel rechts: HTTP,
Client oben,
Server unten

```
010.000.000.115.37895-080.237.227.140.00080: GET / HTTP/1.1
Host: www.linux-magazin.de
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.14) Gecko/20110221
Ubuntu/10.10 (maverick) Firefox/3.6.14
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: __utma_a2a=7292745027.1307663422.1276106496.1289038656.1296989770.7; __u
tma=38187326.1490806165.1276106496.1299494517.1299497866.9; __utmz=38187326.1296
989770.4.4.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=linux%20terminat
or%20anleitung; eZSESSIDlinux_magazin=c52d5a90a4c7c559bde932dbe3d9c401; __utmc=3
8187326; __utmv=; __utmb=38187326.1.10.1299497866
Pragma: no-cache
Cache-Control: no-cache

080.237.227.140.00080-010.000.000.115.37895: HTTP/1.1 200 OK
Date: Mon, 07 Mar 2011 11:38:16 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.14 with Suhosin-Patch proxy_htm
l/3.0.0 mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: eZ Publish
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Mon, 07 Mar 2011 11:38:16 GMT
Served-by: www.linux-magazin.de
Content-language: de-DE
Keep-Alive: timeout=15, max=98
Connection: Keep-Alive
```

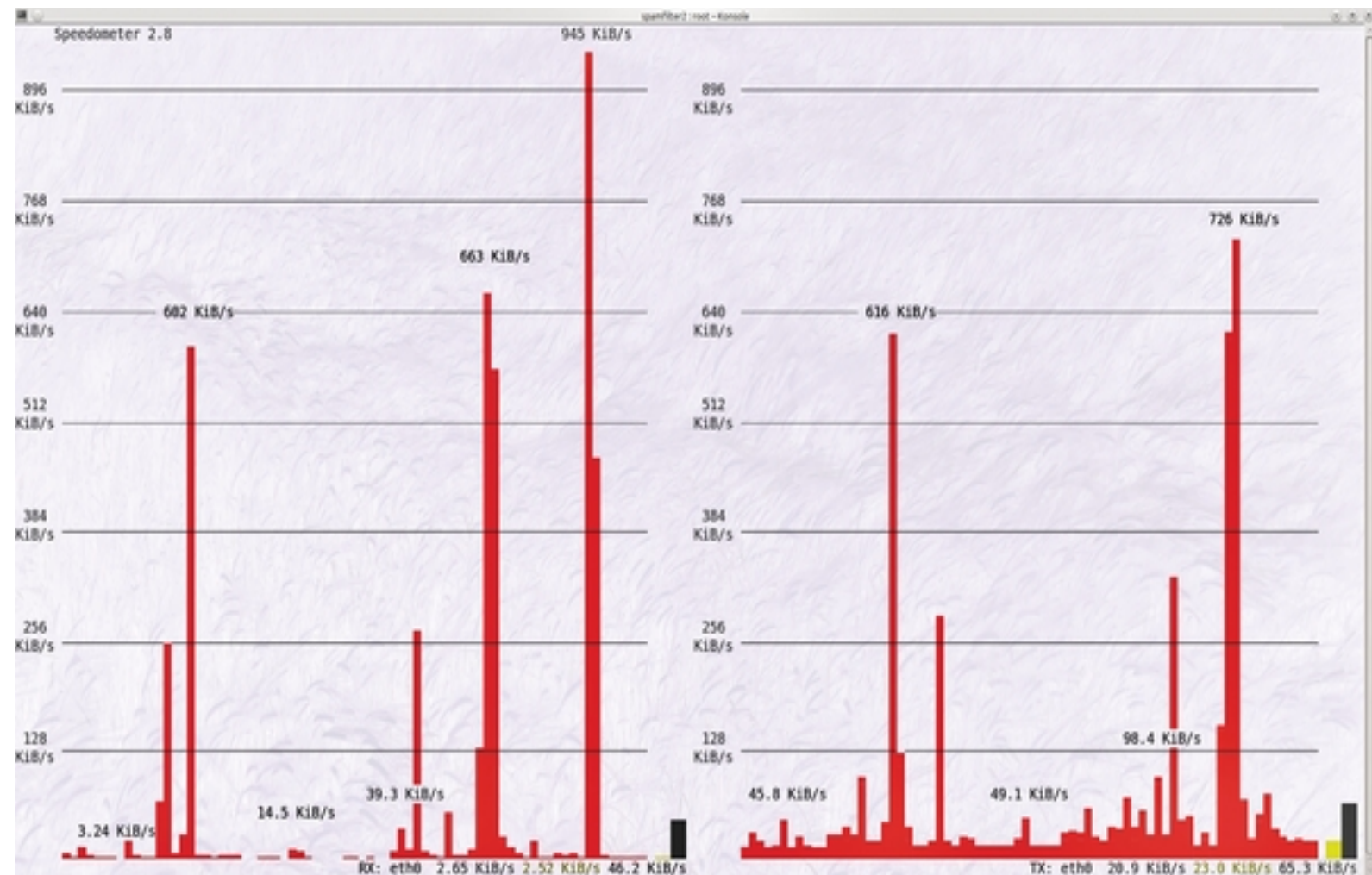

Speedometer

Speedometer zeigt den aktuellen Netzdurchsatz auf der Konsole an.

```
speedometer -s -l  
-tx eth0 -c -rx eth0
```

-c = columns

-l = linear (default: logar.)

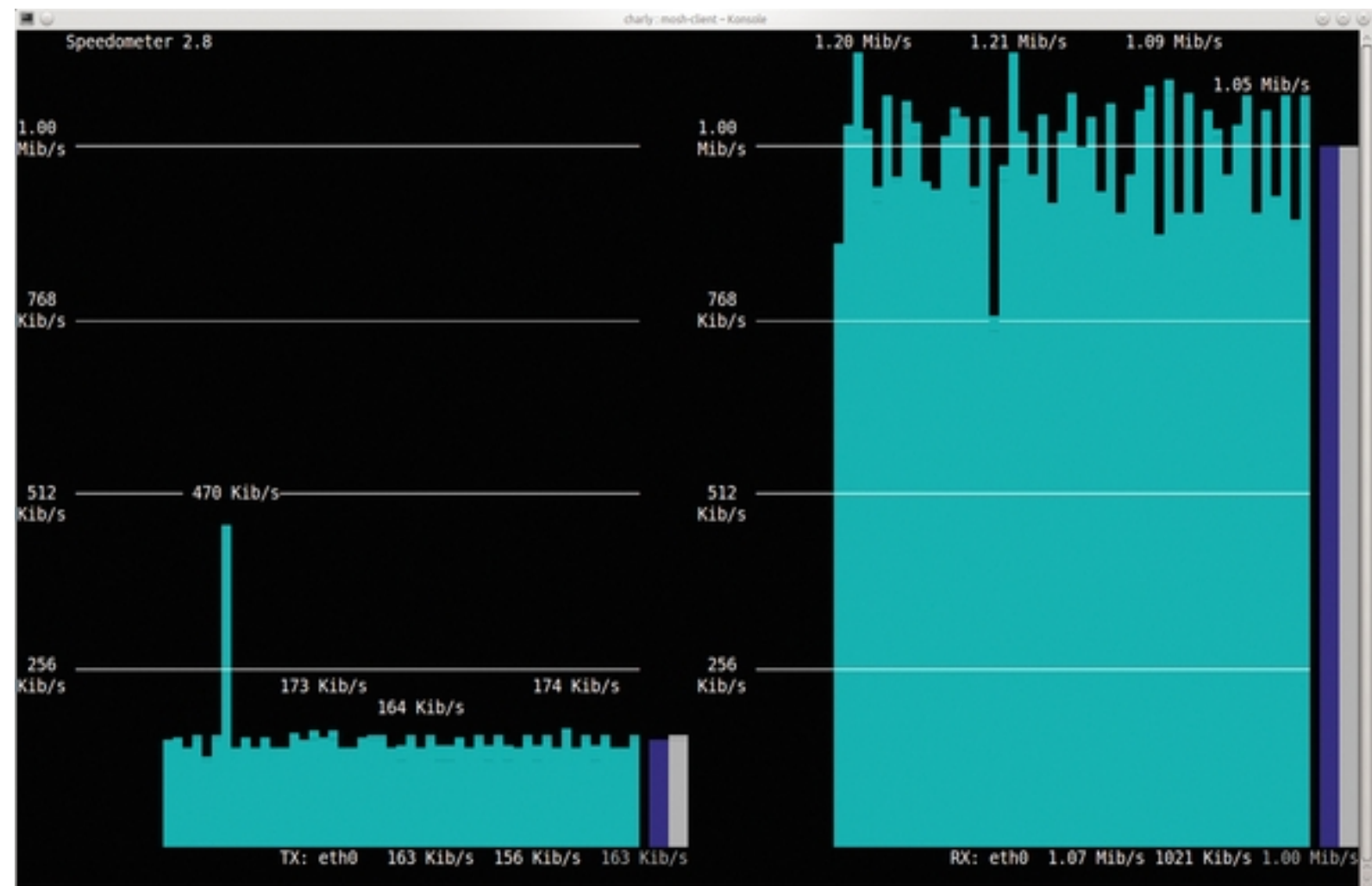


Trickle

Trickle begrenzt die Bandbreite, die ein Prozess verbraten darf.

```
trickle -u 32 -d 256  
firefox
```

- auch als Daemon (trickled)
- in Configfile lassen sich Prioritäten für Protokolle definieren

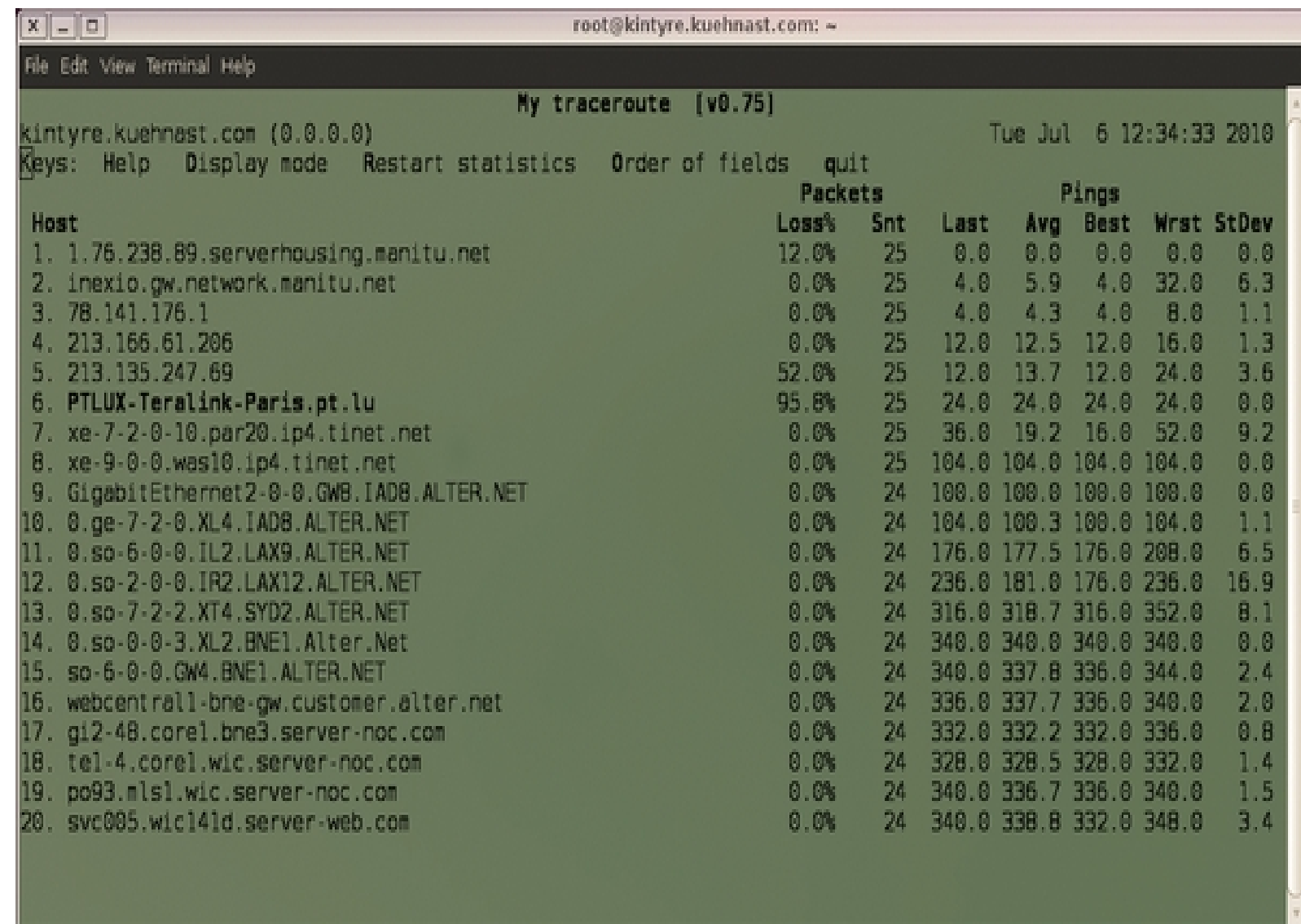


MTR

MTR ist wie traceroute, nur besser.

```
mtr -i5 <Ziel>
```

- Intervall 5 sec
- „-l“ = Rohdaten f. Script
- „-u“ = UDP statt ICMP



My traceroute [v0.75]

kintyre.kuehnast.com (0.0.0.0) Tue Jul 6 12:34:33 2010

Keys: Help Display mode Restart statistics Order of fields quit

Host	Packets		Pings				
	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 1.76.238.89.serverhousing.manitu.net	12.0%	25	0.0	0.0	0.0	0.0	0.0
2. inexist.gw.network.manitu.net	0.0%	25	4.0	5.9	4.0	32.0	6.3
3. 78.141.176.1	0.0%	25	4.0	4.3	4.0	8.0	1.1
4. 213.166.61.206	0.0%	25	12.0	12.5	12.0	16.0	1.3
5. 213.135.247.69	52.0%	25	12.0	13.7	12.0	24.0	3.6
6. PTLUX-Teralink-Paris.pt.lu	95.8%	25	24.0	24.0	24.0	24.0	0.0
7. xe-7-2-0-10.par20.ip4.tinet.net	0.0%	25	36.0	19.2	16.0	52.0	9.2
8. xe-9-0-0.was10.ip4.tinet.net	0.0%	25	104.0	104.0	104.0	104.0	0.0
9. GigabitEthernet2-0-0.GW8.IAD8.ALTER.NET	0.0%	24	100.0	100.0	100.0	100.0	0.0
10. 0.ge-7-2-0.XL4.IAD8.ALTER.NET	0.0%	24	104.0	100.3	100.0	104.0	1.1
11. 0.so-6-0-0.IL2.LAX9.ALTER.NET	0.0%	24	176.0	177.5	176.0	208.0	6.5
12. 0.so-2-0-0.IR2.LAX12.ALTER.NET	0.0%	24	236.0	181.0	176.0	236.0	16.9
13. 0.so-7-2-2.XT4.SYD2.ALTER.NET	0.0%	24	316.0	318.7	316.0	352.0	8.1
14. 0.so-0-0-3.XL2.BNE1.Alter.Net	0.0%	24	340.0	340.0	340.0	340.0	0.0
15. so-6-0-0.GW4.BNE1.ALTER.NET	0.0%	24	340.0	337.8	336.0	344.0	2.4
16. webcentrell-bne-gw.customer.alter.net	0.0%	24	336.0	337.7	336.0	340.0	2.0
17. gi2-48.core1.bne3.server-noc.com	0.0%	24	332.0	332.2	332.0	336.0	0.8
18. tel-4.core1.wic.server-noc.com	0.0%	24	328.0	328.5	328.0	332.0	1.4
19. po93.mls1.wic.server-noc.com	0.0%	24	340.0	336.7	336.0	340.0	1.5
20. svc005.wic141d.server-web.com	0.0%	24	340.0	338.8	332.0	348.0	3.4

ifdata: Schnittstellen mundgerecht serviert

Ifdata liefert Informationen zu Schnittstellen zur Weiterverarbeitung in Shellscripts.

```
if $(ifdata -e eth0); then
    echo "Interface gefunden"; [...]
else
    echo "Interface nicht gefunden"; [...]
fi

$ ifdata -p eth0      [oder »-pa« , »-pn« , »-pb«, »-pm«]
10.0.0.106 255.255.255.0 10.0.0.255 1500

$ ifdata -soe eth0 # Error counter auslesen
```

Schwerer Missbrauch: Netzdiagnose mit `lsof`

Alles ist ein File, und `lsof` zeigt sie alle an. Auch wenn es Sockets sind.

Alle Verbindungen auf Port 22 anzeigen:

```
lsof -i :22
```

Alle ausgehenden Verbindungen zu example.com anzeigen:

```
lsof -i@example.com
```

Alle ausgehenden SSH-Verbindungen zu example.com anzeigen, die der User „Charly“ aufgebaut hat:

```
lsof -a -u charly -i@example.com:22
```


Swaks: Mailserver-Diagnose

Swaks exerziert den SMTP-Dialog bis zu einem definierbaren Punkt durch.

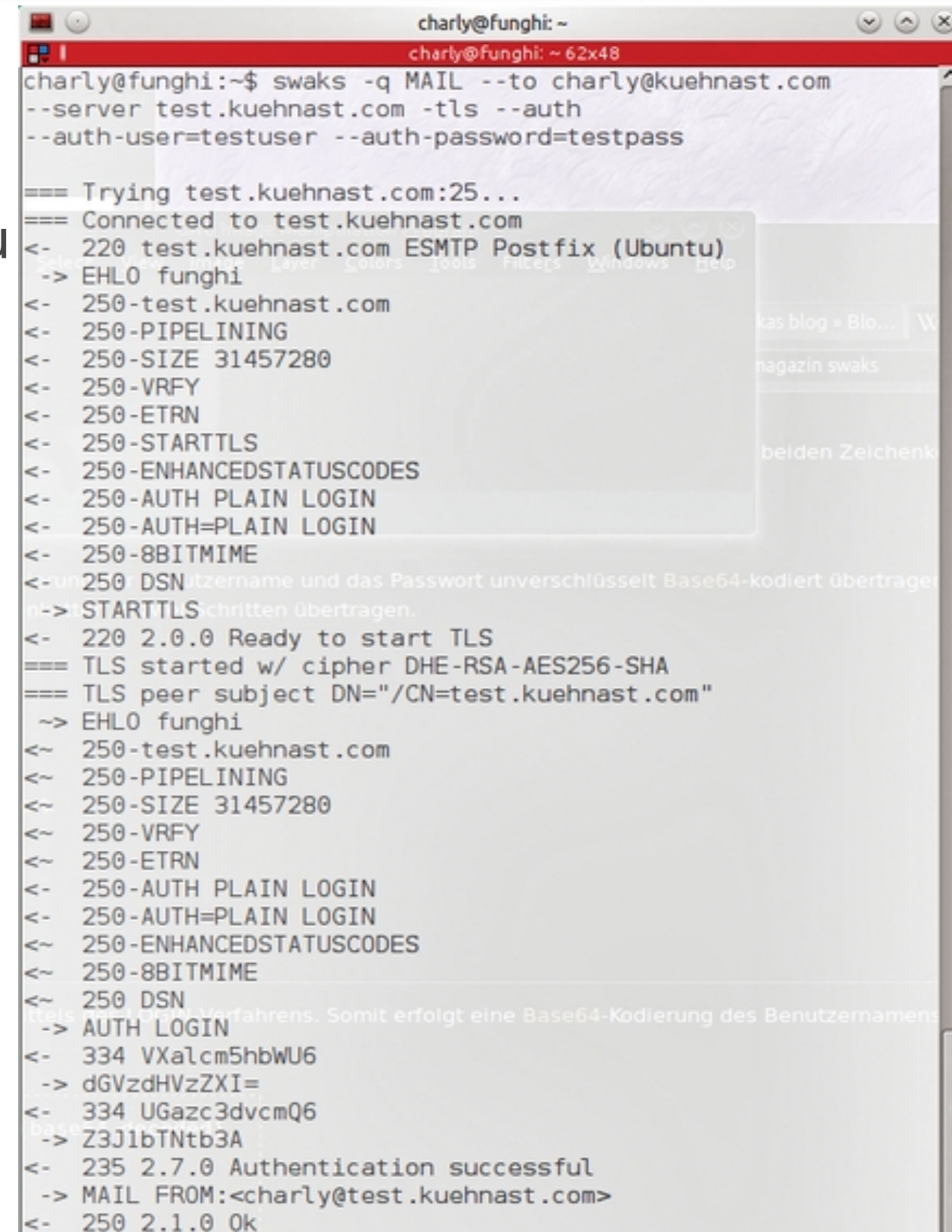
swaks

--from=charly@kuehnast.com

--to=charly@example.com -

server=mail.example.com

„-q RCPT“ stoppt SMTP-
Dialog nach RCPT



```
charly@funghi: ~  
charly@funghi: ~ 62x48  
charly@funghi:~$ swaks -q MAIL --to charly@kuehnast.com  
--server test.kuehnast.com -tls --auth  
--auth-user=testuser --auth-password=testpass  
  
=== Trying test.kuehnast.com:25...  
=== Connected to test.kuehnast.com  
<- 220 test.kuehnast.com ESMTP Postfix (Ubuntu)  
-> EHLO funghi  
<- 250-test.kuehnast.com  
<- 250-PIPELINING  
<- 250-SIZE 31457280  
<- 250-VRFY  
<- 250-ETRN  
<- 250-STARTTLS  
<- 250-ENHANCEDSTATUSCODES  
<- 250-AUTH PLAIN LOGIN  
<- 250-AUTH=PLAIN LOGIN  
<- 250-8BITMIME  
<-un 250 DSN  
n->STARTTLS  
<- 220 2.0.0 Ready to start TLS  
=== TLS started w/ cipher DHE-RSA-AES256-SHA  
=== TLS peer subject DN="/CN=test.kuehnast.com"  
-> EHLO funghi  
<- 250-test.kuehnast.com  
<- 250-PIPELINING  
<- 250-SIZE 31457280  
<- 250-VRFY  
<- 250-ETRN  
<- 250-AUTH PLAIN LOGIN  
<- 250-AUTH=PLAIN LOGIN  
<- 250-ENHANCEDSTATUSCODES  
<- 250-8BITMIME  
<- 250 DSN  
-> AUTH LOGIN  
<- 334 VXalcm5hbWU6  
-> dGVzdHVzZXI=  
<- 334 UGazc3dvcmQ6  
-> Z3J1bTNTb3A  
<- 235 2.7.0 Authentication successful  
-> MAIL FROM:<charly@test.kuehnast.com>  
<- 250 2.1.0 Ok
```


SPL – Shakespeare Programming Language

Caesar, a successful and soon dead roman emperor

Othello, a venetian general

Act I: A battle of words

Scene I: Caesar insults Othello

[Enter Caesar and Othello]

Caesar: You stupid rotten beggar!

Open your heart!

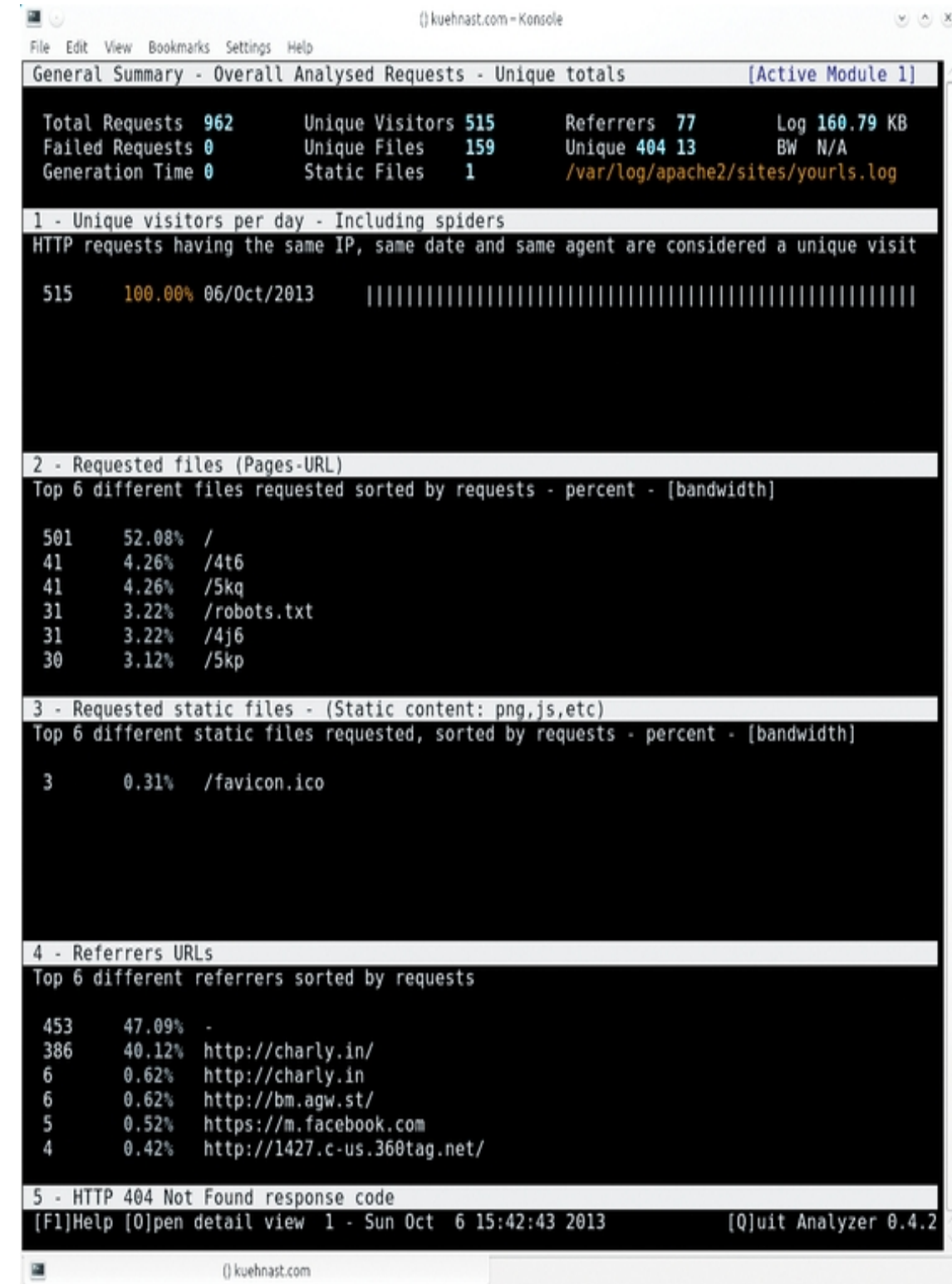
Speak your mind!

GoAccess: Logmittel

GoAccess analysiert Webserver-Logfiles in Echtzeit.

```
goaccess -f  
/var/log/apache2/  
access.log
```

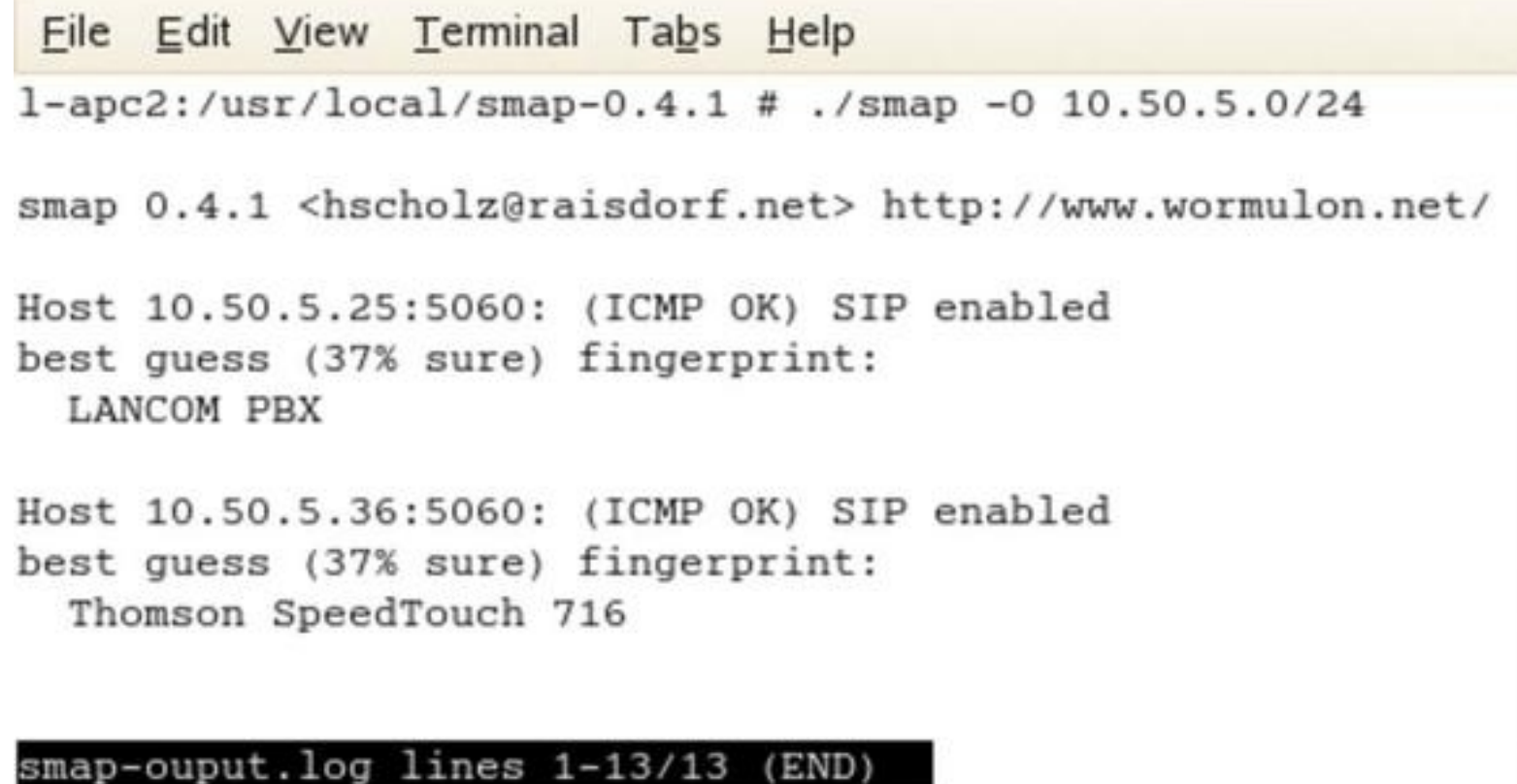
```
“-e <IP>” = ignore
```



Smap

Nmap für VoIP

- findet VoIP-Devices im LAN
- Syntax ähnlich Nmap
- Fingerprinting
- Lernmodus



The screenshot shows a terminal window with a menu bar (File, Edit, View, Terminal, Tabs, Help). The command executed is `l-apc2:/usr/local/smap-0.4.1 # ./smap -O 10.50.5.0/24`. The output shows the version of Smap (0.4.1) and the source URL (<http://www.wormulon.net/>). It then displays two scan results for hosts 10.50.5.25 and 10.50.5.36, both on port 5060. The first host is identified as a LANCOM PBX, and the second as a Thomson SpeedTouch 716. At the bottom, a status bar indicates the log file path and line count: `smap-ouput.log lines 1-13/13 (END)`.

```
File Edit View Terminal Tabs Help
l-apc2:/usr/local/smap-0.4.1 # ./smap -O 10.50.5.0/24

smap 0.4.1 <hscholz@raisdorf.net> http://www.wormulon.net/

Host 10.50.5.25:5060: (ICMP OK) SIP enabled
best guess (37% sure) fingerprint:
  LANCOM PBX

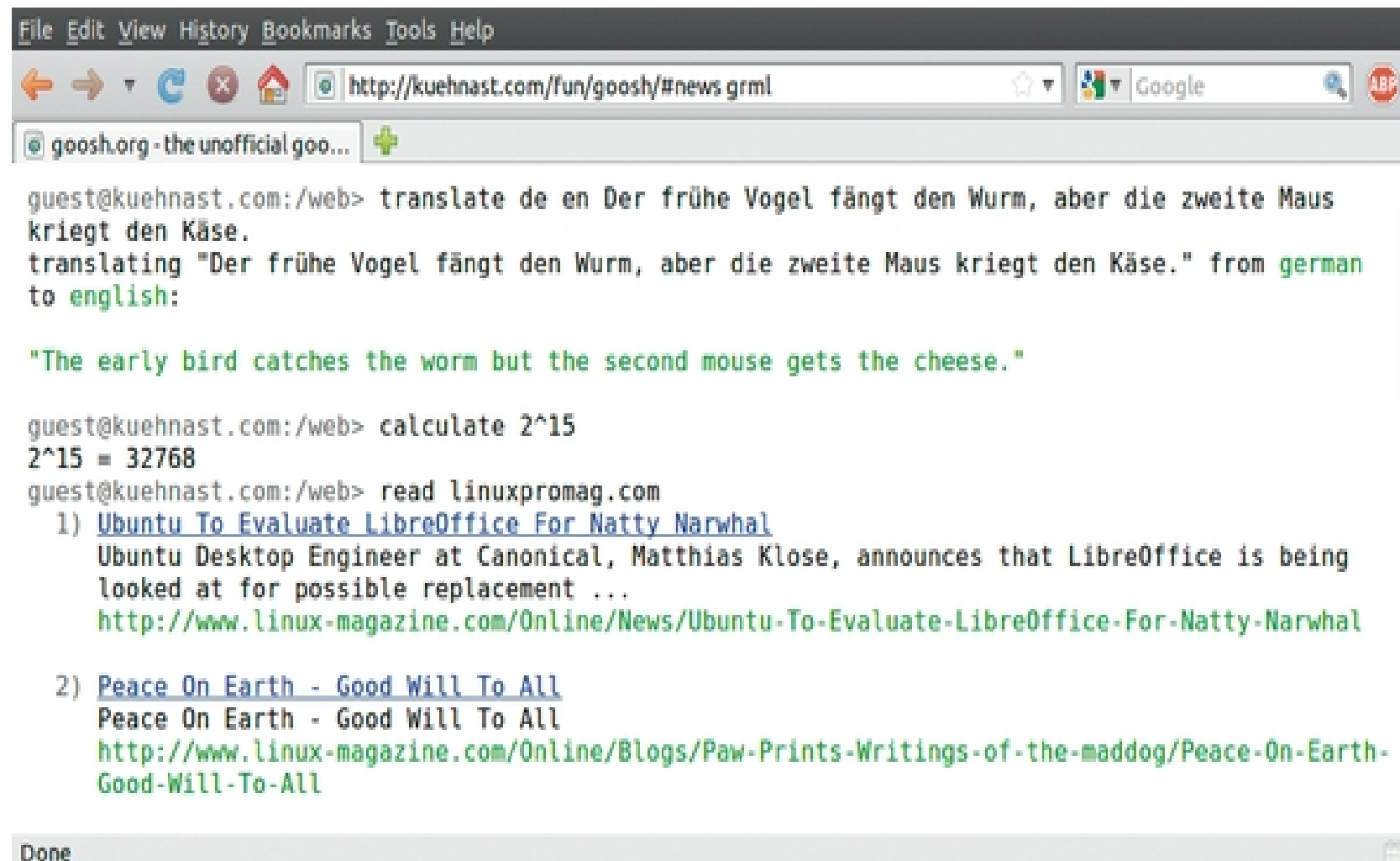
Host 10.50.5.36:5060: (ICMP OK) SIP enabled
best guess (37% sure) fingerprint:
  Thomson SpeedTouch 716

smap-ouput.log lines 1-13/13 (END)
```


Goosh

Google in a (nut)shell

- Textmode-Google
- Shortcuts zu Bilder-, Blog, Wiki-Suche uvm
- Google Translator
- RSS



```
File Edit View History Bookmarks Tools Help
http://kuehnast.com/fun/goosh/#news grml
goosh.org - the unofficial goo...
guest@kuehnast.com:/web> translate de en Der frühe Vogel fängt den Wurm, aber die zweite Maus
kriegt den Käse.
translating "Der frühe Vogel fängt den Wurm, aber die zweite Maus kriegt den Käse." from german
to english:

"The early bird catches the worm but the second mouse gets the cheese."

guest@kuehnast.com:/web> calculate 2^15
2^15 = 32768
guest@kuehnast.com:/web> read linuxpromag.com
1) Ubuntu To Evaluate LibreOffice For Natty Narwhal
   Ubuntu Desktop Engineer at Canonical, Matthias Klose, announces that LibreOffice is being
   looked at for possible replacement ...
   http://www.linux-magazine.com/Online/News/Ubuntu-To-Evaluate-LibreOffice-For-Natty-Narwhal

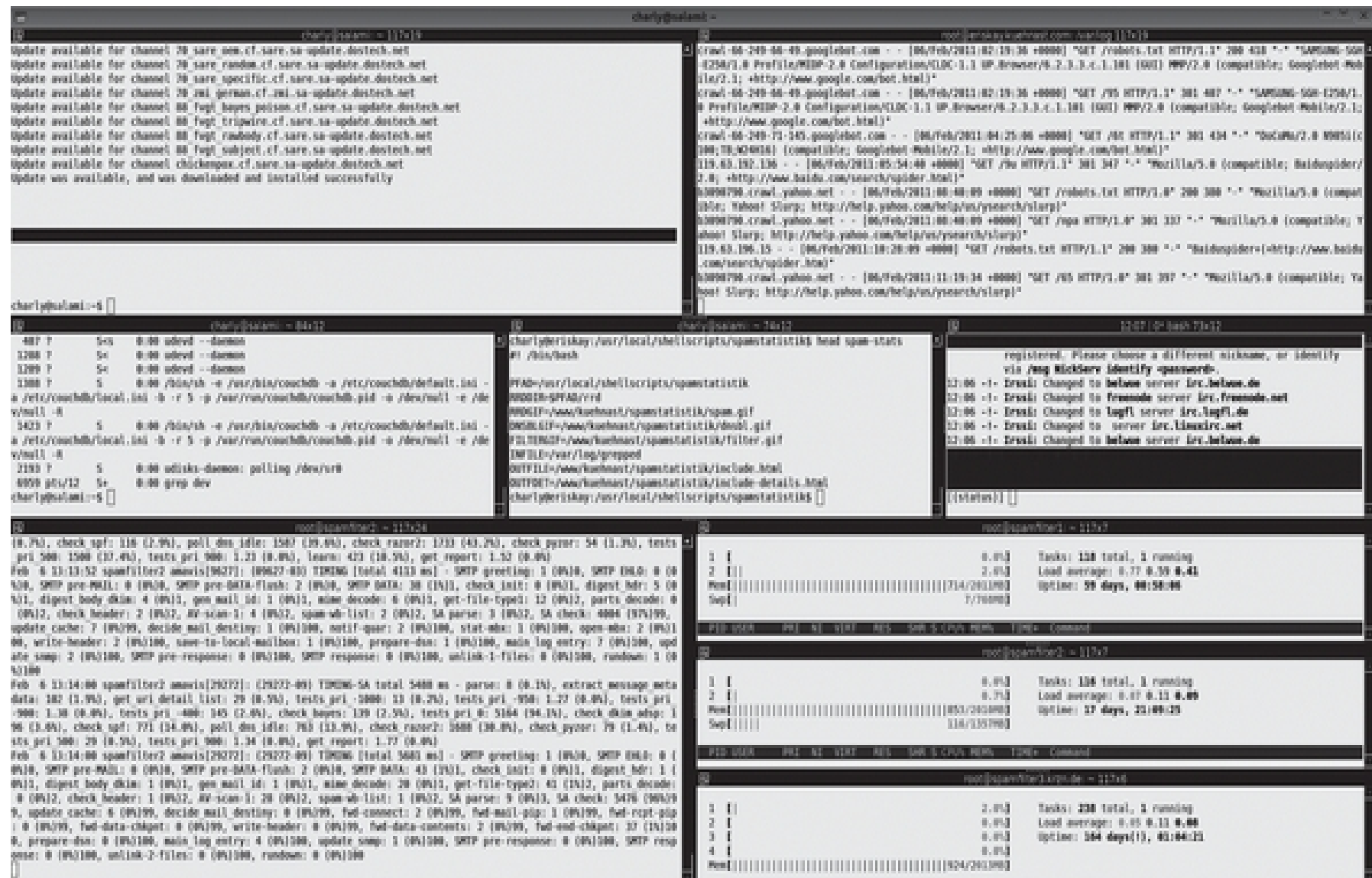
2) Peace On Earth - Good Will To All
   Peace On Earth - Good Will To All
   http://www.linux-magazine.com/Online/Blogs/Paw-Prints-Writings-of-the-maddog/Peace-On-Earth-Good-Will-To-All

Done
```

Terminator

Terminator ist ein Film ein Konsolenmultiplexer für grafische Oberflächen

- Einfache Tastaturkommandos
- „Zoomen“
- Drag to reorder
- Vollbildmodus
- Cooler Name

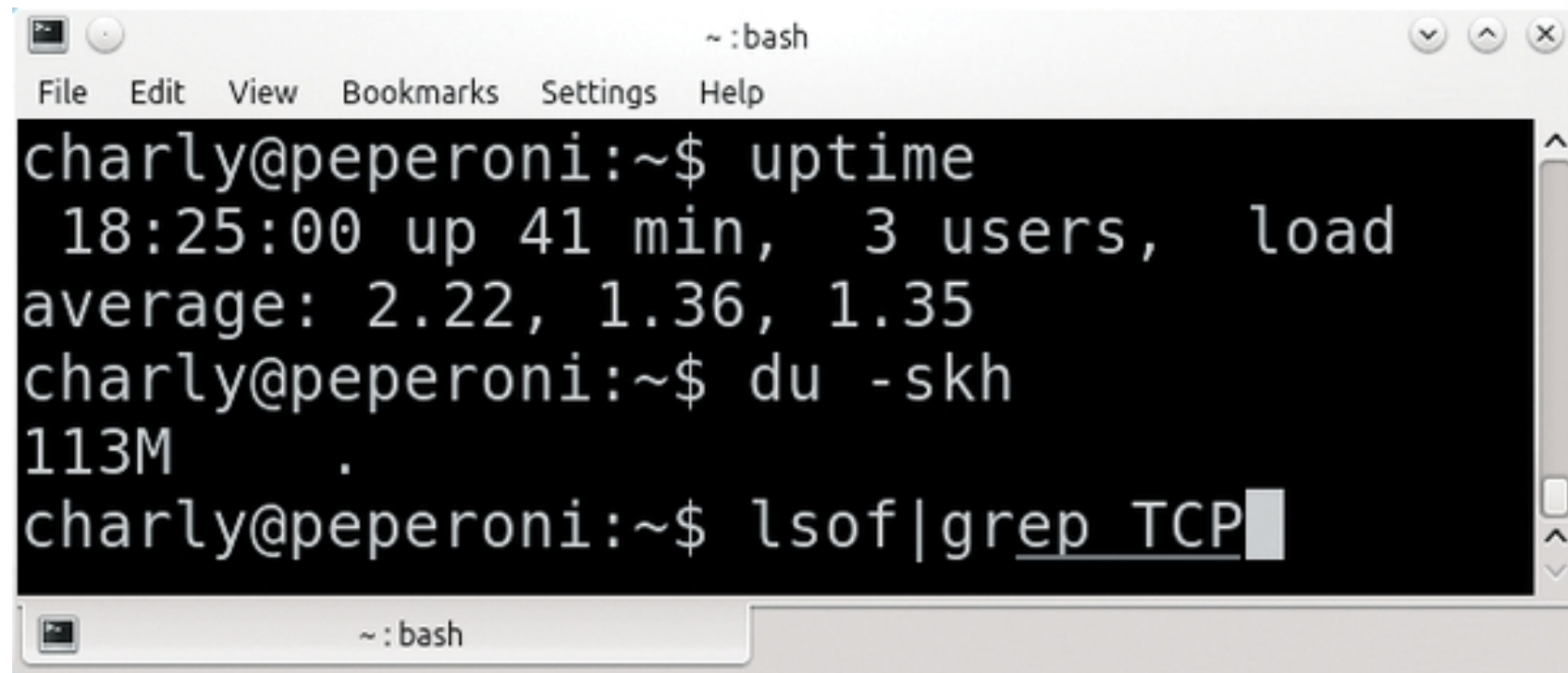


The screenshot displays the Terminator application, a terminal multiplexer. It features a dark-themed interface with several windows. The top window shows a list of update notifications for various channels. Below it, there are several smaller windows, each displaying different types of data: a list of system processes, a log of network connections, a list of tasks, and a list of files. The interface is designed to be efficient, allowing users to manage multiple terminal sessions simultaneously using simple keyboard shortcuts.

Mosh

Mosh ist ein SSH-Ersatz für schlechte Verbindungsqualität

- Verbindungsaufbau über TCP, danach UDP
- Verbindungen sind extrem langlebig und überstehen sogar Wechsel der Client-IP und Reisen mit der Deutschen Bahn

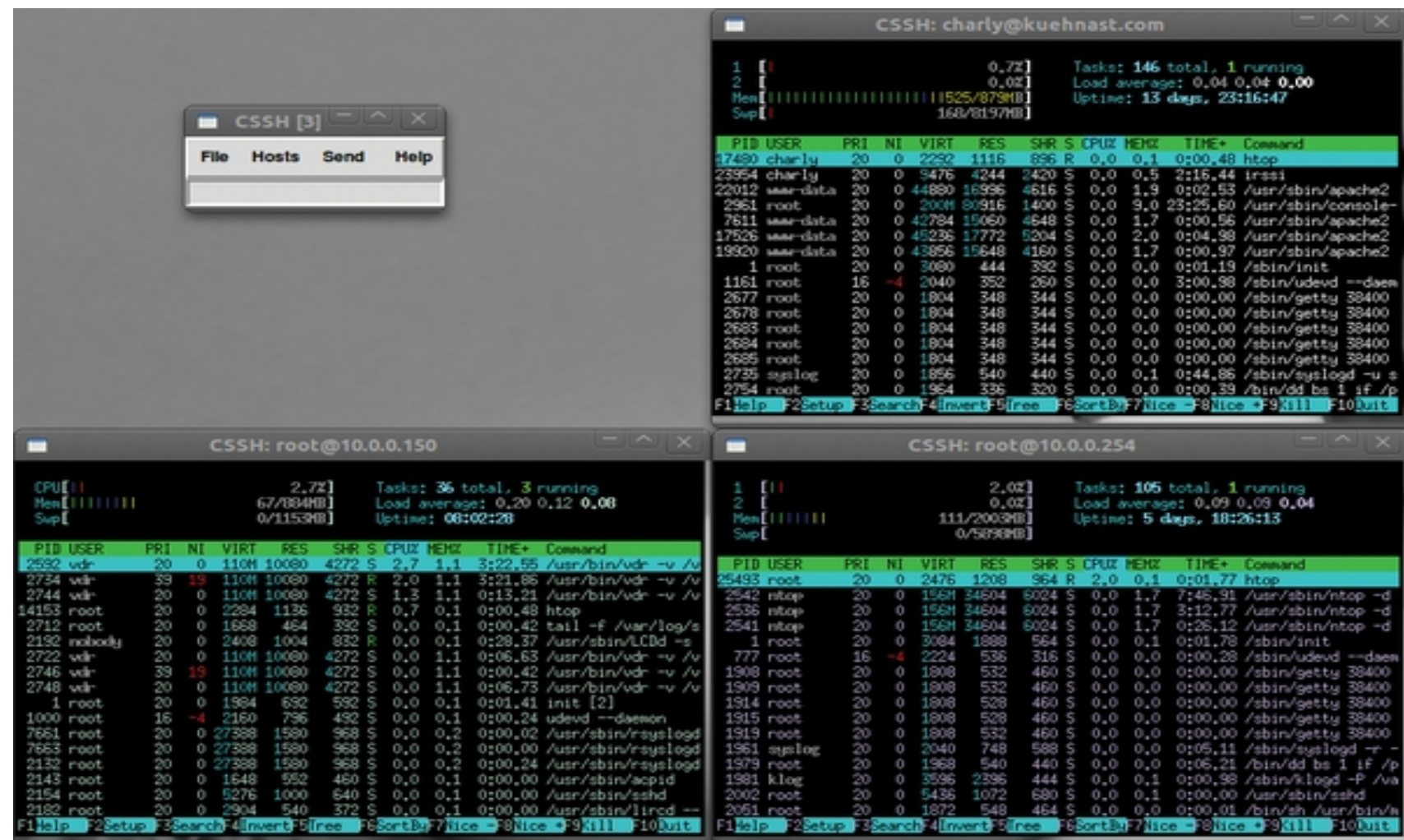


```
~ : bash
File Edit View Bookmarks Settings Help
charly@peperoni:~$ uptime
 18:25:00 up 41 min,  3 users,  load
average: 2.22, 1.36, 1.35
charly@peperoni:~$ du -skh
113M      .
charly@peperoni:~$ lsof|grep TCP
```

ClusterSSH

Den gleichen Fehler auf beliebig vielen Servern gleichzeitig machen

- Kommando einmal eingeben, wird auf n Server ausgeführt
- Möglichkeit, Gruppen zu definieren
- Zwei Themes: „light“ und „dark“



Unscharf, aber cool: tre-agrep

Tre-agrep ist wie grep mit einstellbarer Unschärfe

```
tre-agrep -2  
<wort> <file>
```

Findet „wort“ in „file“ mit
bis zu 2 Zeichen
Anabweichung

Ideal zum Aufspüren von
Tippfehlern in Logs



```
charly@funghi: ~  
charly@funghi:~$ tre-agrep -2 example.com /var/log/mail.log  
[...]  
Jul 31 14:14:01 eriskay amavis[26132]: (26132-05) FWD via SMTP: <charly@kueh  
.com> -> <user1@exmaple.com>, BODY=7BIT 250 2.0.0 from MTA([127.0.0.1]:10025)  
0 2.0.0 Ok: queued as 0980B888422  
  
Jul 31 14:14:01 eriskay amavis[26132]: (26132-05) Passed CLEAN, <charly@kueh  
.com> -> <user1@exmaple.com>, Message-ID: <20120731141354.BB5B0888421@kuehna  
om>, mail_id: lqCtUEEvEg7x, Hits: -1.901, size: 324, queued_as: 0980B888422.  
6 ms  
  
Jul 31 14:14:01 eriskay postfix/smtp[15227]: BB5B0888421: to=<user1@exmaple.  
, relay=127.0.0.1[127.0.0.1]:10024, delay=6.3, delays=0.02/0/0/6.3, dsn=2.0.  
tatus=sent (250 2.0.0 from MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as (0  
888422)  
[...]  
charly@funghi:~$
```

QPS

QPS ist ps, top und lsof in einem grafischen Tool

COMMAND	PID	TTY	USER	NICE	STAT	RSS	%MEM	%CPU	START	TIME	COMMAND_LINE
irqbalance	1110	-	root	0	S	636K	0.02	0.00	08:49	2.59s	irqbalance
openvpn	1129	-	root	0	S	1M	0.05	0.00	08:49	0.26s	openvpn --writepid /var/run/openvpn
openvpn	1155	-	root	0	S	3M	0.11	0.00	08:49	0:54	openvpn --writepid /var/run/openvpn
exim4	1419	-	Debian-exim	0	S	1008K	0.03	0.00	08:49	0:00s	exim4 -bd -q30m
tleds	1475	-	root	10	S N	388K	0.01	0.00	08:49	0:23	tleds -c -q -d 100 eth0
bluetoothd	1503	-	root	0	S	1M	0.05	0.00	08:49	0:00s	bluetoothd
apache2	1619	-	root	0	S	6M	0.20	0.00	08:50	0:34s	apache2 -k start
apache2	1624	-	www-data	0	S	3M	0.12	0.00	08:50	0:00s	apache2 -k start
apache2	1625	-	www-data	0	S	3M	0.12	0.00	08:50	0:00s	apache2 -k start
apache2	1626	-	www-data	0	S	3M	0.12	0.00	08:50	0:00s	apache2 -k start
apache2	1627	-	www-data	0	S	3M	0.12	0.00	08:50	0:00s	apache2 -k start
apache2	1628	-	www-data	0	S	3M	0.12	0.00	08:50	0:00s	apache2 -k start
g15stats	1704	-	root	0	S	1M	0.04	0.00	08:50	1:20	g15stats -s -i eth0 -nsa
getty	1707	1	root	0	S	528K	0.02	0.00	08:50	0:00s	getty -8 38400 tty1
console-kit-daemon	1796	-	root	0	S	3M	0.10	0.00	08:56	0:03s	console-kit-daemon --no-daemon
dbus-launch	1919	-	charly	0	S	496K	0.01	0.00	08:56	0:00s	dbus-launch --exit-with-session x-ses
dbus-daemon	1920	-	charly	0	S	2M	0.07	0.00	08:56	3.27s	dbus-daemon --fork --print-pid 5 --pr
udisks-daemon	1951	-	root	0	S	3M	0.10	0.00	08:56	0:42s	udisks-daemon
udisks-daemon	1952	-	root	0	S	724K	0.02	0.00	08:56	0:76s	udisks-daemon: polling /dev/sr0 >>

Total Process : 212

Bestes Feature: zeigt übersichtlich alle Dateien an, die ein bestimmter Prozess gerade im Zugriff hat

Pen

Einfacher Loadbalancer, in zwei Minuten konfiguriert

Kommandozeile:

```
pen 80 www1:8000:100 www2:80:100
```

Oder als Daemon:

```
MAX_CONNECTIONS=500
```

```
PORT=80
```

```
BACKEND=2
```

```
SERVER1=10.0.0.51:80
```

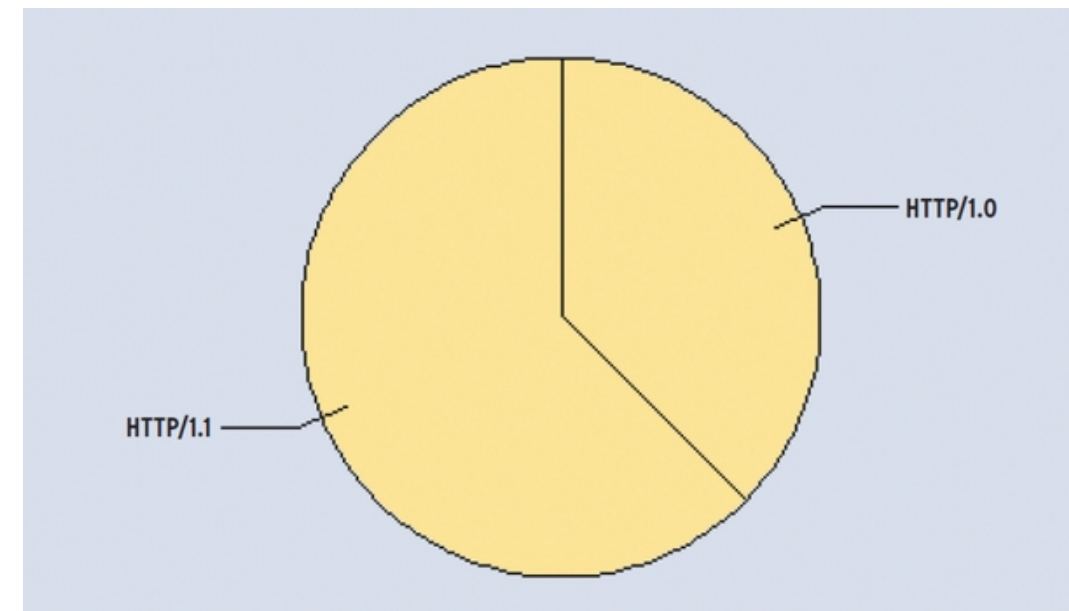
```
SERVER2=10.0.0.52:80
```

Lire

Lire ist ein Logauswerter mit Plugins für ca. 40 Logformate

Lire unterstützt

- sechs verschiedene Mailserver
- Bind
- Tiny DNS
- Snort
- div. Webserver
- MySQL und PostgreSQL
- Spamassassin
- ...



Robot	Requests	% Total
Yahoo! Slurp	76	41,1
BaiDuSpider	43	23,2
MSNBot	35	18,9
Google (http://www.google.com/)	29	15,7
larbin	2	1,1
Total for 185 records	185	100,0

Ttytter

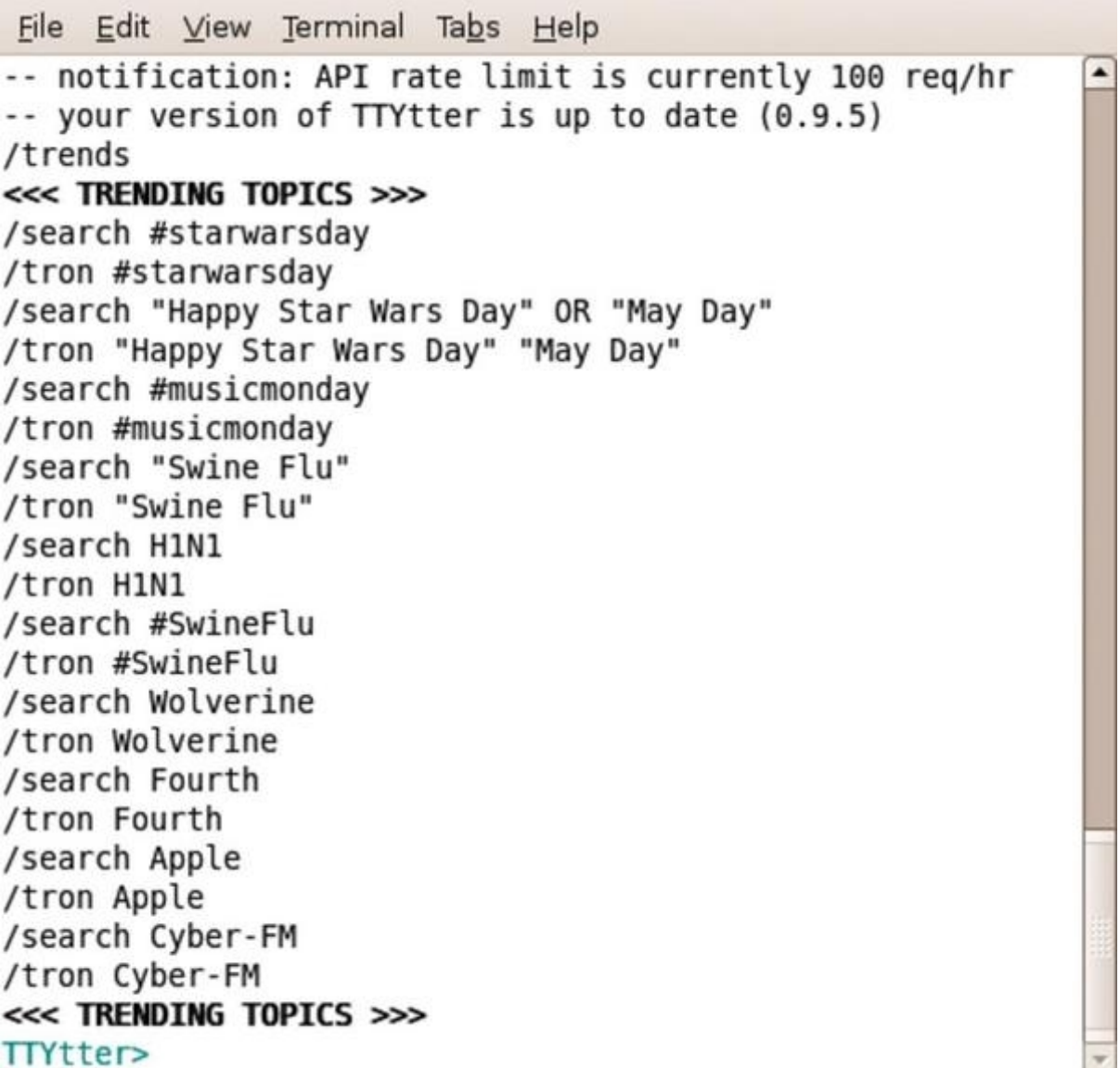
Nichtgrafischer Twitter-Client

Ttytter starten:

```
ttytter -vcheck -ansi -wrap  
-user=Username:Passwort
```

Tweets direkt über die Twitter-API absetzen:

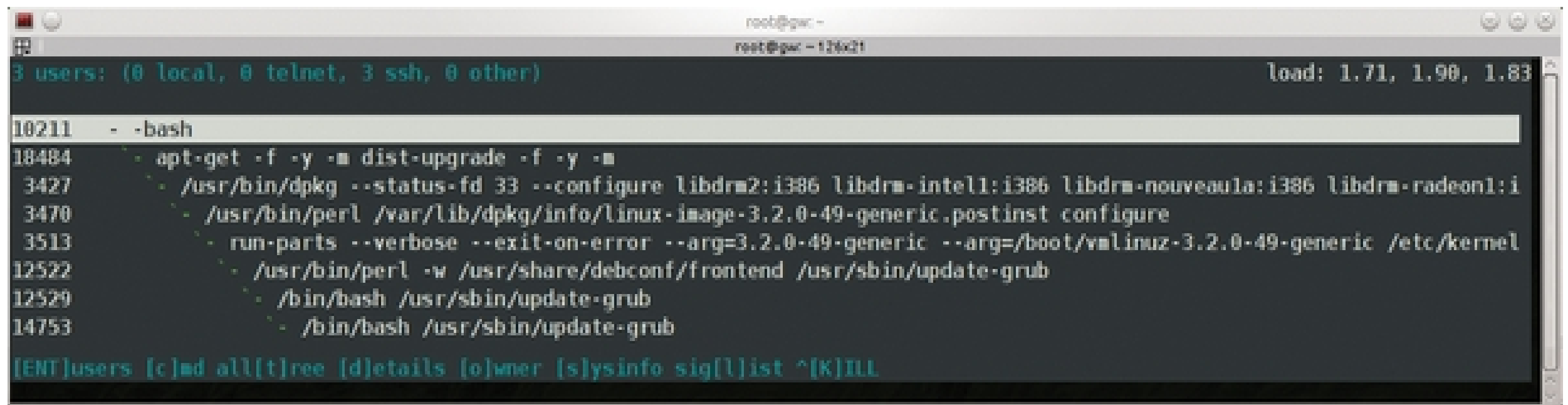
```
curl --basic --user  
"User:Passwort" --data-ascii  
"Blafasel"  
"http://twitter.com/statuses/  
update.json"
```



```
File Edit View Terminal Tabs Help  
-- notification: API rate limit is currently 100 req/hr  
-- your version of TTYtter is up to date (0.9.5)  
/trends  
<<< TRENDING TOPICS >>>  
/search #starwarsday  
/tron #starwarsday  
/search "Happy Star Wars Day" OR "May Day"  
/tron "Happy Star Wars Day" "May Day"  
/search #musicmonday  
/tron #musicmonday  
/search "Swine Flu"  
/tron "Swine Flu"  
/search H1N1  
/tron H1N1  
/search #SwineFlu  
/tron #SwineFlu  
/search Wolverine  
/tron Wolverine  
/search Fourth  
/tron Fourth  
/search Apple  
/tron Apple  
/search Cyber-FM  
/tron Cyber-FM  
<<< TRENDING TOPICS >>>  
TTYtter>
```

Whowatch

Whowatch liefert Informationen darüber, wer was von wo aus macht.



```
root@gw: ~
root@gw: ~ 12:02:11
3 users: (0 local, 0 telnet, 3 ssh, 0 other) load: 1.71, 1.90, 1.83
10211 - -bash
18484   - apt-get -f -y -m dist-upgrade -f -y -m
3427   - /usr/bin/dpkg --status-fd 33 --configure libdrm2:i386 libdrm-intell:i386 libdrm-nouveau:i386 libdrm-radeon:i386
3470   - /usr/bin/perl /var/lib/dpkg/info/linux-image-3.2.0-49-generic.postinst configure
3513   - run-parts --verbose --exit-on-error --arg=3.2.0-49-generic --arg=/boot/vmlinuz-3.2.0-49-generic /etc/kernel
12522   - /usr/bin/perl -w /usr/share/debconf/frontend /usr/sbin/update-grub
12529   - /bin/bash /usr/sbin/update-grub
14753   - /bin/bash /usr/sbin/update-grub
[ENT]users [c]md all[t]ree [d]etails [o]wner [s]ysinfo sig[l]ist ^[K]ILL
```

Prozesse werden als Baumstruktur angezeigt (ähnlich pstree). Interaktiv können Informationen wie Prozessdetails, Owner, Laufzeit etc. abgerufen werden.

W3AF

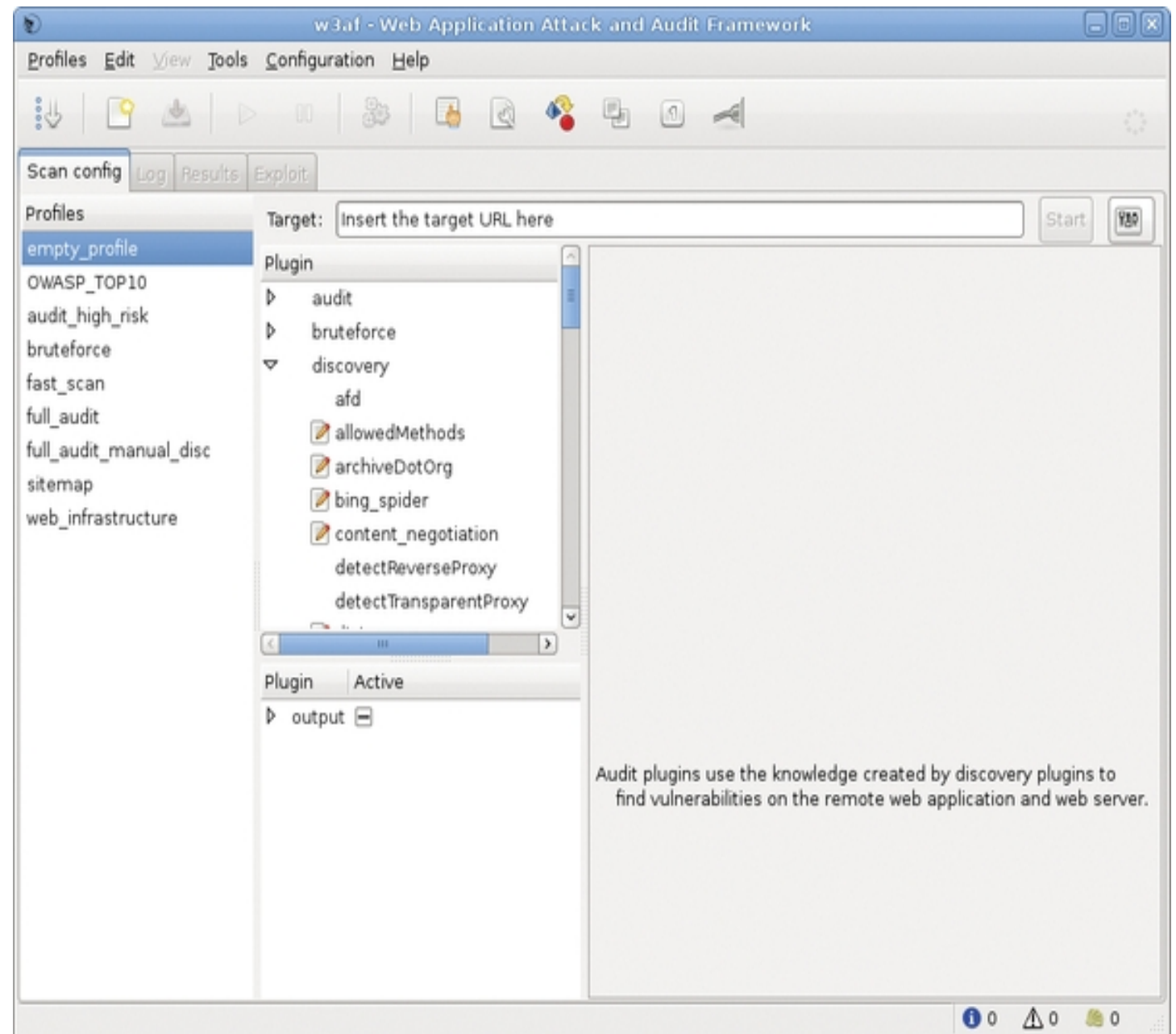
Web Application Attack and Audit Framework

W3AF findet gängigste
Schwachstellen in Websites:

- XSS
- SQL Injection

Es beherrscht Evasion-
Techniken, um IDS/IPS zu
verwirren.

Nicht so umfangreich wie
OpenVAS oder Metasploit.



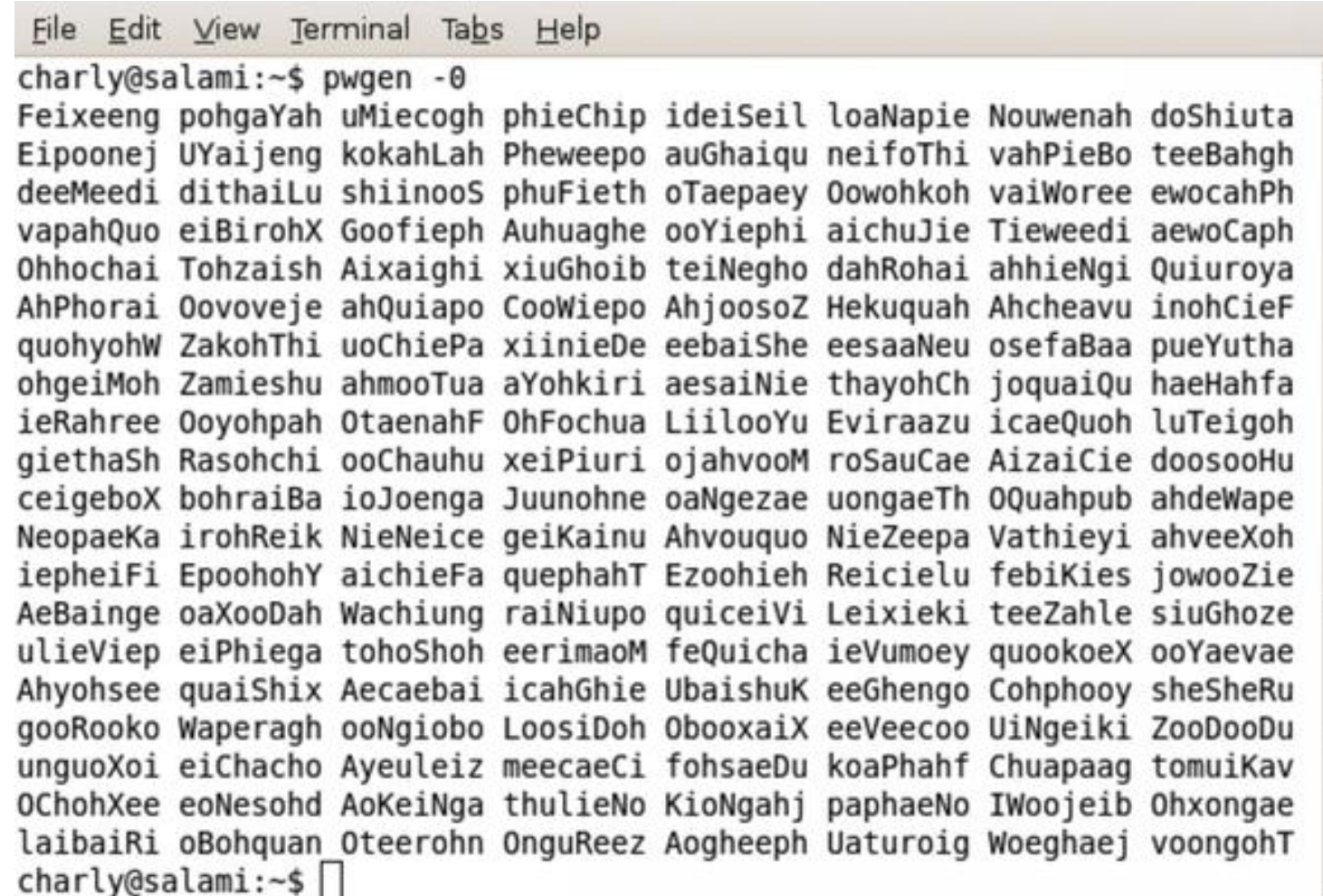
pwgen

Generiert Passwörter in wählbarer Komplexität

pwgen -s -y :

+3HEg,_51P.A@=2U@||{}9Cy

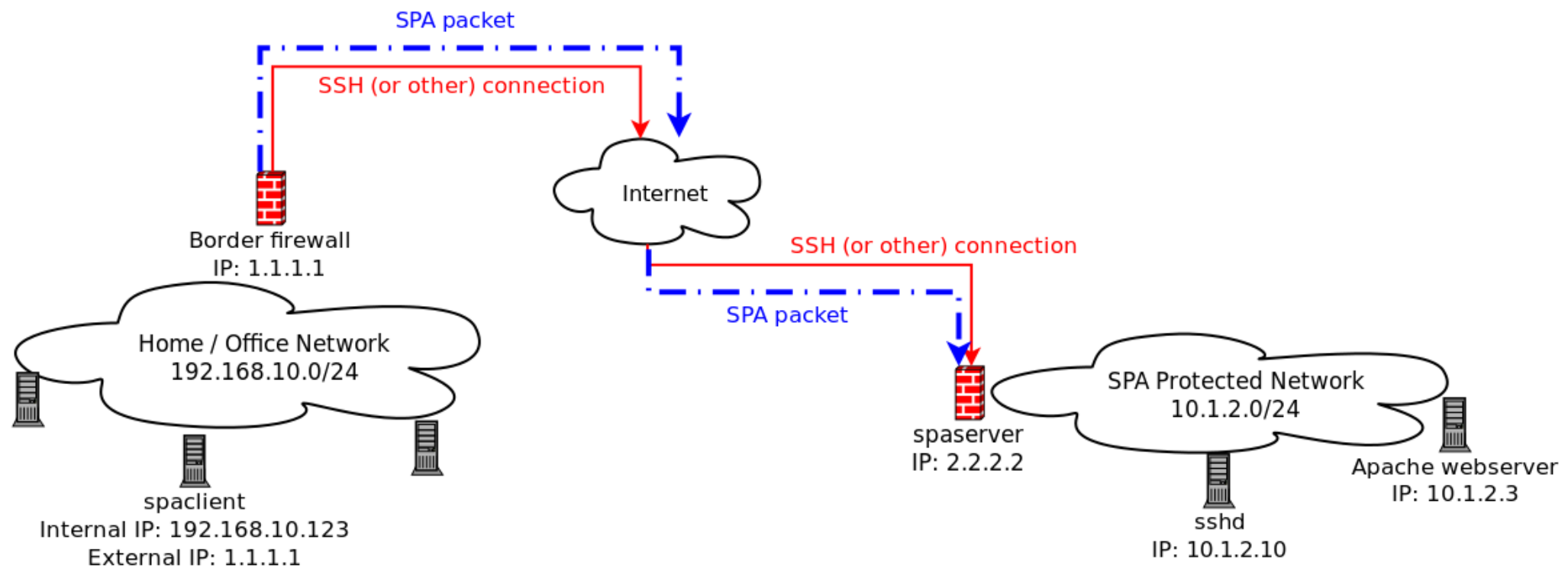
Parameter „-B“ unterdrückt
leicht verwechselbare Zeichen
wie 0 und O oder 1 und l.



```
File Edit View Terminal Tabs Help
charly@salami:~$ pwgen -0
Feixeeng pohgaYah uMiecogh phieChip ideiSeil loaNapie Nouwenah doShiuta
Eipoonej UYaijeng kokahLah Pheweepo auGhaiqu neifoThi vahPieBo teeBahgh
deeMeedi dithaiLu shiinooS phuFieth oTaepaey Oowohkoh vaiWoree ewocahPh
vapahQuo eiBirohX Goofieph Auhuaghe ooYiephi aichuJie Tieweedi aewoCaph
Ohhochai Tohzaish Aixaighi xiuGhoib teiNegho dahRohai ahhieNgi Quiuroya
AhPhorai Oovoveje ahQuiapo Coowiepo AhjoosoZ Hekuquah Ahcheavu inohCieF
quohyohW ZakohThi uoChiePa xiinieDe eebaiShe eesaaNeu osefaBaa pueYutha
ohgeiMoh Zamieshu ahmooTua aYohkiri aesaiNie thayohCh joquaiQu haeHahfa
ieRahree Ooyohpah OtaenahF OhFochua LiilooYu Eviraazu icaeQuoh luTeigoh
giethaSh Rasohchi ooChauhu xeiPiuri ojahvooM roSauCae AizaiCie doosooHu
ceigeboX bohraiBa ioJoenga Juunohne oanGezae uongaeTh OQuahpub ahdeWape
NeopaeKa irohReik NieNeice geiKainu Ahvouquo NieZeepa Vathieyi ahveeXoh
iepheiFi EpooohohY aichieFa quephahT Ezoochieh Reicielu febiKies jowooZie
AeBainge oaXooDah Wachiung raiNiupo quiceivi Leixieki teeZahle siuGhoze
ulieViep eiPhiega tohoShoh eerimaoM feQuicha ieVumoeY quookoeX ooYaevae
Ahyohsee quaiShix Aeceabai icaHghie UbaishuK eeGhengo Cohphooy sheSheRu
gooRooko Waperagh ooNgiobo LoosiDoh ObooxaiX eeVeecoo UiNgeiki ZooDooDu
unguoXoi eiChacho Ayeuleiz meecaeCi fohsaeDu koaPhahf Chuapaag tomuiKav
OChohXee eoNesohd AoKeiNga thulieNo KioNgahj paphaeNo IWoosjeib Ohxongae
laibaiRi oBohquan Oteerohn OnguReez Aogheeph Uaturoig Woeghaej voongohT
charly@salami:~$
```


Single Packet Authentication mit Fwknop

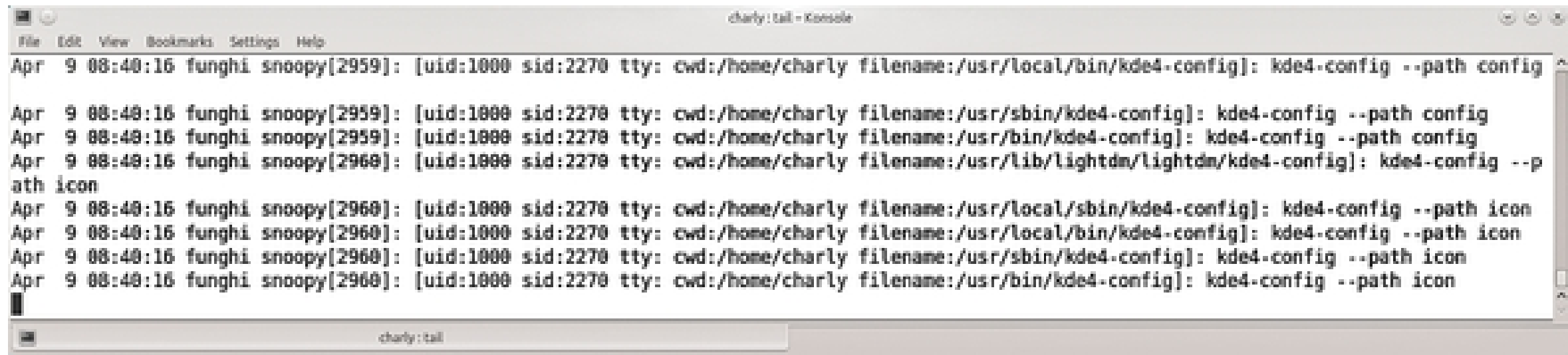
Die bessere Alternative zu Port Knocking



- Client schickt ein einziges verschlüsseltes Paket an der Server. Server öffnet nach Prüfung einen bestimmten Port (zB 22).
- unterstützt auch asymmetrische Ciphers, zB 2048-Bit ElGamal GPG-Keys

Snoopy

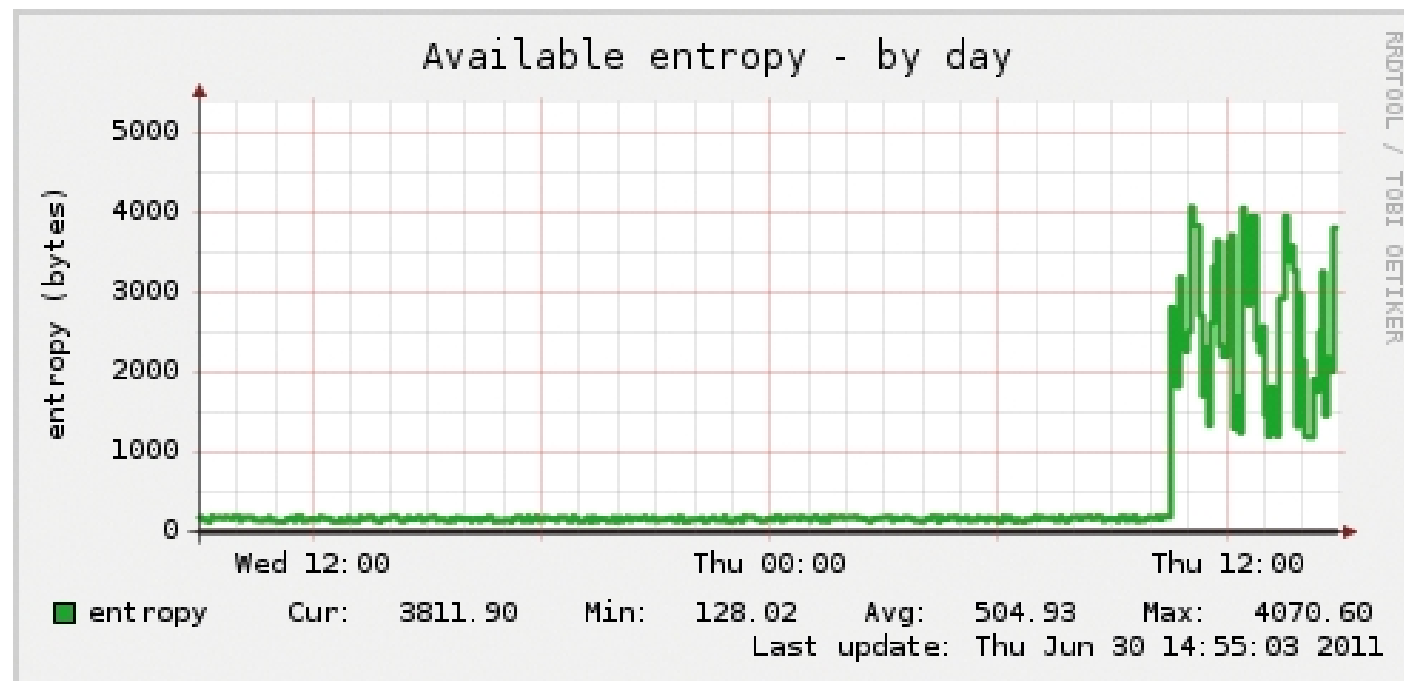
Gedächtnisstütze, Ergänzung zur Bash-History



```
charly: tail - Konsole
File Edit View Bookmarks Settings Help
Apr 9 08:48:16 funghi snoopy[2959]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/local/bin/kde4-config]: kde4-config --path config
Apr 9 08:48:16 funghi snoopy[2959]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/sbin/kde4-config]: kde4-config --path config
Apr 9 08:48:16 funghi snoopy[2959]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/bin/kde4-config]: kde4-config --path config
Apr 9 08:48:16 funghi snoopy[2960]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/lib/lightdm/lightdm/kde4-config]: kde4-config --p
ath icon
Apr 9 08:48:16 funghi snoopy[2960]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/local/sbin/kde4-config]: kde4-config --path icon
Apr 9 08:48:16 funghi snoopy[2960]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/local/bin/kde4-config]: kde4-config --path icon
Apr 9 08:48:16 funghi snoopy[2960]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/sbin/kde4-config]: kde4-config --path icon
Apr 9 08:48:16 funghi snoopy[2960]: [uid:1000 sid:2270 tty: cwd:/home/charly filename:/usr/bin/kde4-config]: kde4-config --path icon
```

- Wrapper um `execve()`
- `LD_Preload`
- schreibt jedes ausgeführte Kommando nach `/var/log/auth.log`
- läßt sich auf Kommandos einschränken, die von UID 0 ausgeführt wurden
- ignoriert Navigation im Dateisystem (`cd`, ...)

HavegeD sorgt für Unordnung



- keine Parameter. Starten und das Chaos kommt sofort.
- erste Hilfe bei zickigem hostapd (*"deauthenticated due to local deauth request"*)

SSLScan

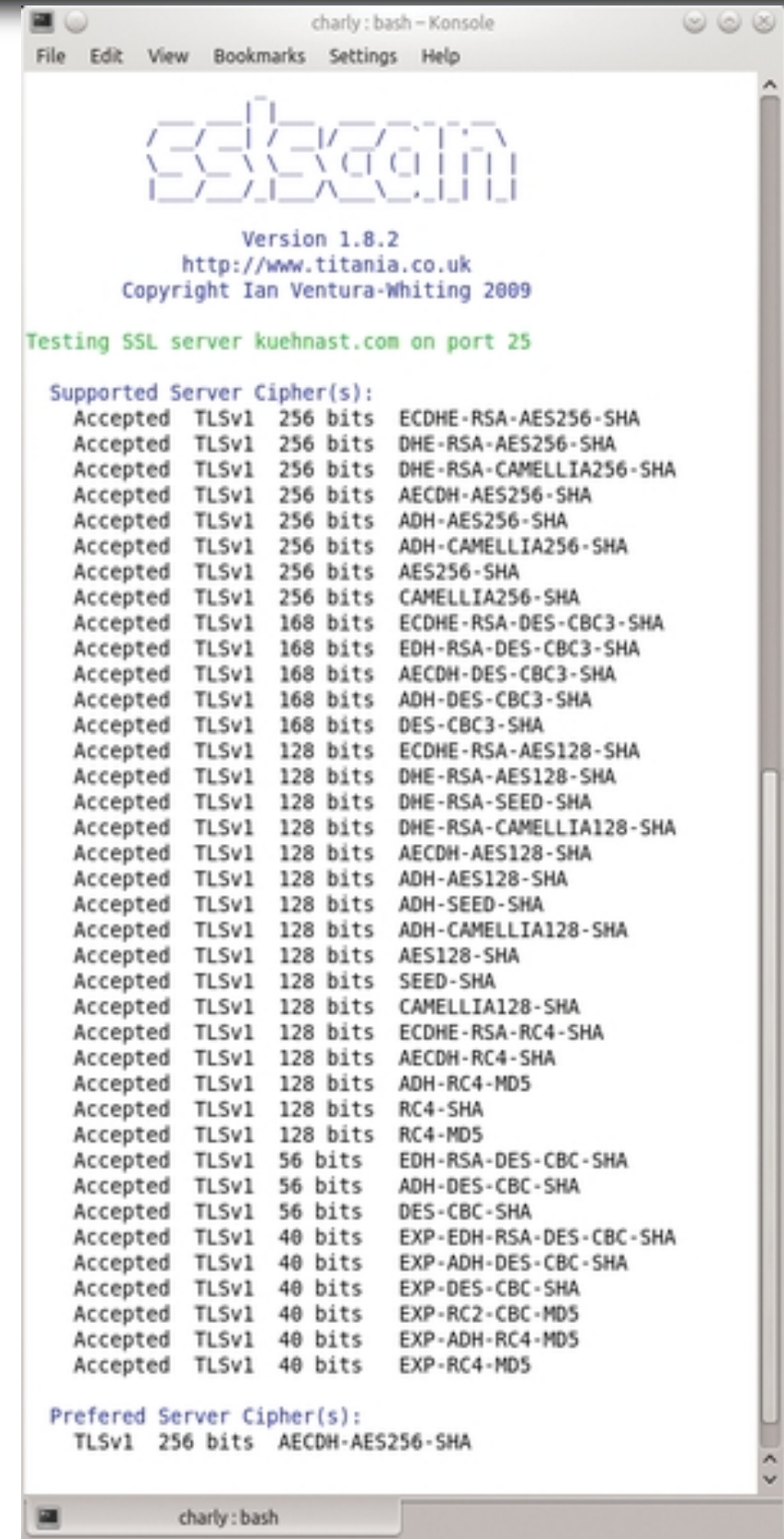
Findet heraus, welche Ciphers ein Server unterstützt (HTTPS und SMTP)

Alle TLS-Ciphers, die der Server akzeptiert:

```
sslscan -no-failed --tls1  
www.example.com
```

Das gleiche für SMTP:

```
sslscan --no-failed --starttls  
--tlsv1 kuehnast.com:25
```



```
charly: bash - Konsole
File Edit View Bookmarks Settings Help

  sslscan

Version 1.8.2
http://www.titania.co.uk
Copyright Ian Ventura-Whiting 2009

Testing SSL server kuehnast.com on port 25

Supported Server Cipher(s):
Accepted TLSv1 256 bits ECDHE-RSA-AES256-SHA
Accepted TLSv1 256 bits DHE-RSA-AES256-SHA
Accepted TLSv1 256 bits DHE-RSA-CAMELLIA256-SHA
Accepted TLSv1 256 bits AECDH-AES256-SHA
Accepted TLSv1 256 bits ADH-AES256-SHA
Accepted TLSv1 256 bits ADH-CAMELLIA256-SHA
Accepted TLSv1 256 bits AES256-SHA
Accepted TLSv1 256 bits CAMELLIA256-SHA
Accepted TLSv1 168 bits ECDHE-RSA-DES-CBC3-SHA
Accepted TLSv1 168 bits EDH-RSA-DES-CBC3-SHA
Accepted TLSv1 168 bits AECDH-DES-CBC3-SHA
Accepted TLSv1 168 bits ADH-DES-CBC3-SHA
Accepted TLSv1 168 bits DES-CBC3-SHA
Accepted TLSv1 128 bits ECDHE-RSA-AES128-SHA
Accepted TLSv1 128 bits DHE-RSA-AES128-SHA
Accepted TLSv1 128 bits DHE-RSA-SEED-SHA
Accepted TLSv1 128 bits DHE-RSA-CAMELLIA128-SHA
Accepted TLSv1 128 bits AECDH-AES128-SHA
Accepted TLSv1 128 bits ADH-AES128-SHA
Accepted TLSv1 128 bits ADH-SEED-SHA
Accepted TLSv1 128 bits ADH-CAMELLIA128-SHA
Accepted TLSv1 128 bits AES128-SHA
Accepted TLSv1 128 bits SEED-SHA
Accepted TLSv1 128 bits CAMELLIA128-SHA
Accepted TLSv1 128 bits ECDHE-RSA-RC4-SHA
Accepted TLSv1 128 bits AECDH-RC4-SHA
Accepted TLSv1 128 bits ADH-RC4-MD5
Accepted TLSv1 128 bits RC4-SHA
Accepted TLSv1 128 bits RC4-MD5
Accepted TLSv1 56 bits EDH-RSA-DES-CBC-SHA
Accepted TLSv1 56 bits ADH-DES-CBC-SHA
Accepted TLSv1 56 bits DES-CBC-SHA
Accepted TLSv1 40 bits EXP-EDH-RSA-DES-CBC-SHA
Accepted TLSv1 40 bits EXP-ADH-DES-CBC-SHA
Accepted TLSv1 40 bits EXP-DES-CBC-SHA
Accepted TLSv1 40 bits EXP-RC2-CBC-MD5
Accepted TLSv1 40 bits EXP-ADH-RC4-MD5
Accepted TLSv1 40 bits EXP-RC4-MD5

Preferred Server Cipher(s):
TLSv1 256 bits AECDH-AES256-SHA
```


HTPDate

Die ekligste Art, die Systemzeit zu stellen

Zeitstempel aus HTTP-Headern auslesen:

```
HTTP/1.1 404 Not Found
```

```
Date: Mon, 12 May 2014 18:36:09 GMT
```

```
Server: Apache/2.2.22 (Ubuntu)
```

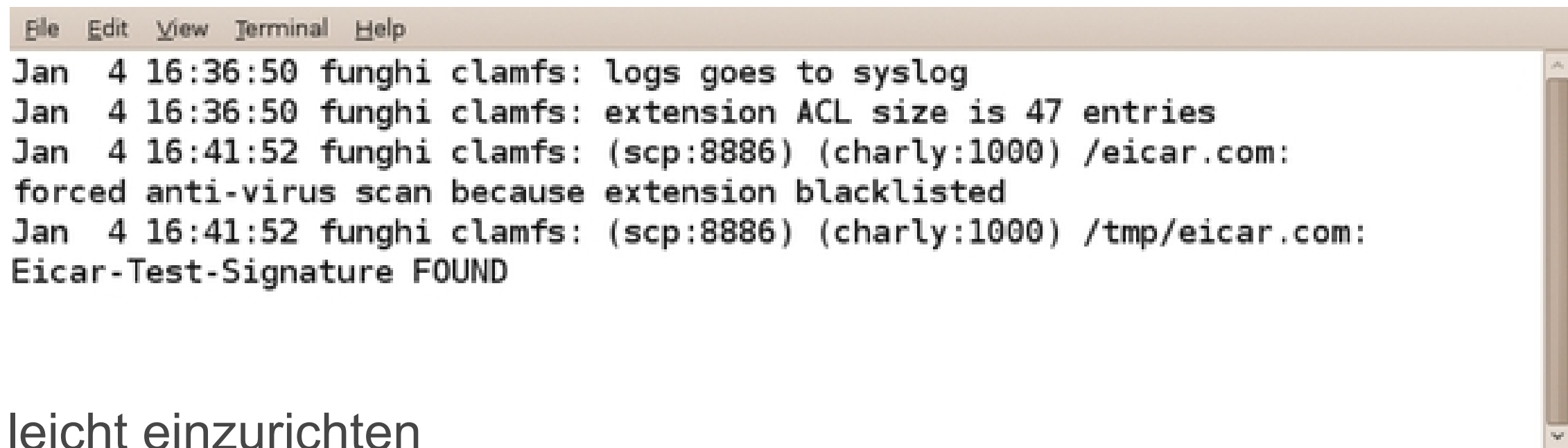
```
Vary: Accept-Encoding
```

Zeit setzen:

```
htpdate -dq -P proxyIP:proxyPORT httpSERVER
```

ClamFS

Userspace-Filesystem integriertem Virenschutz durch ClamAV

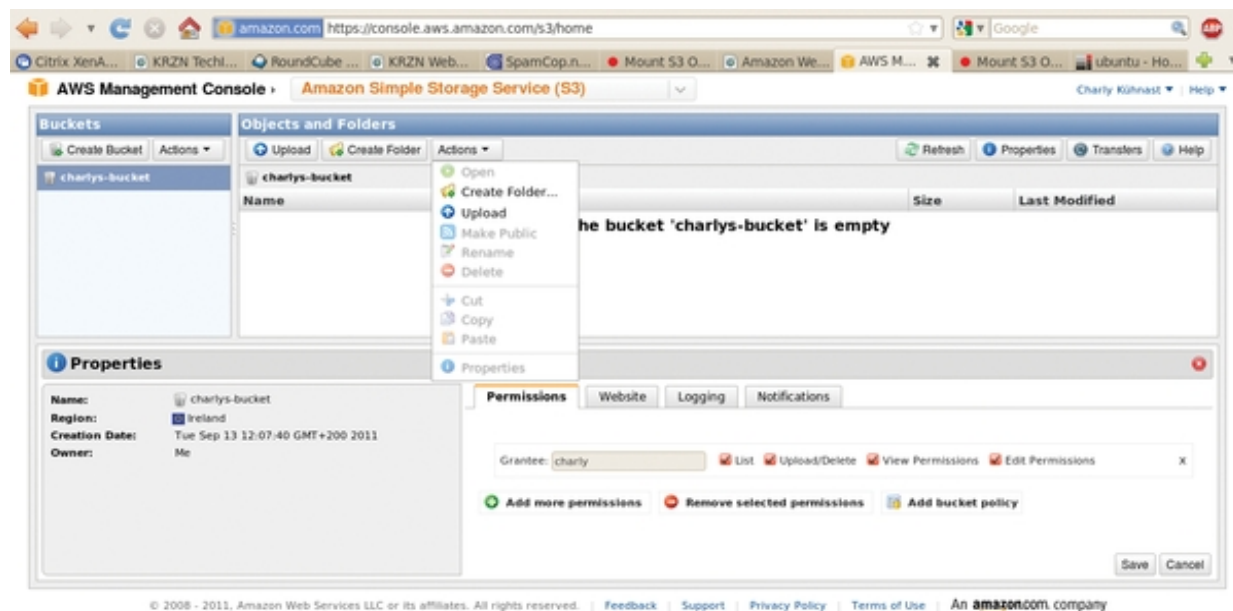
A terminal window with a menu bar (File, Edit, View, Terminal, Help) and a scroll bar on the right. The terminal displays log messages from ClamFS. The messages show the system logging to syslog, the ACL size, and a forced anti-virus scan for a file from eicar.com, which was found to be a test signature.

```
File Edit View Terminal Help
Jan  4 16:36:50 funghi clamfs: logs goes to syslog
Jan  4 16:36:50 funghi clamfs: extension ACL size is 47 entries
Jan  4 16:41:52 funghi clamfs: (scp:8886) (charly:1000) /eicar.com:
forced anti-virus scan because extension blacklisted
Jan  4 16:41:52 funghi clamfs: (scp:8886) (charly:1000) /tmp/eicar.com:
Eicar-Test-Signature FOUND
```

- leicht einzurichten
- miese Performance
- macht Windows-Usern ein warmes Gefühl im Bauch.

S3QL: Daten im Eimer

Userspace-Filesystem, das auf Amazon S3 speichert



- leicht einzurichten
- miese Performance
- flexibel
- für ein Offshore-Backup relativ preiswert
- verschlüsselt

di

df auf Steroiden (und willkommen in der Parameterhöhle).

Alle Dateisysteme:

```
di -a
```

Alle „richtigen“ Dateisysteme:

```
di -a -x proc,tmpfs,fuse
```

Füllstand aller ext4-partitionen in Prozent (und nur das):

```
di -dH -I ext4 -n -f p
```

Alles Informationen über alle ext4-Partitionen als kommaseparierte Liste:

```
di -dh -I ext4 -n -c
```

Durep

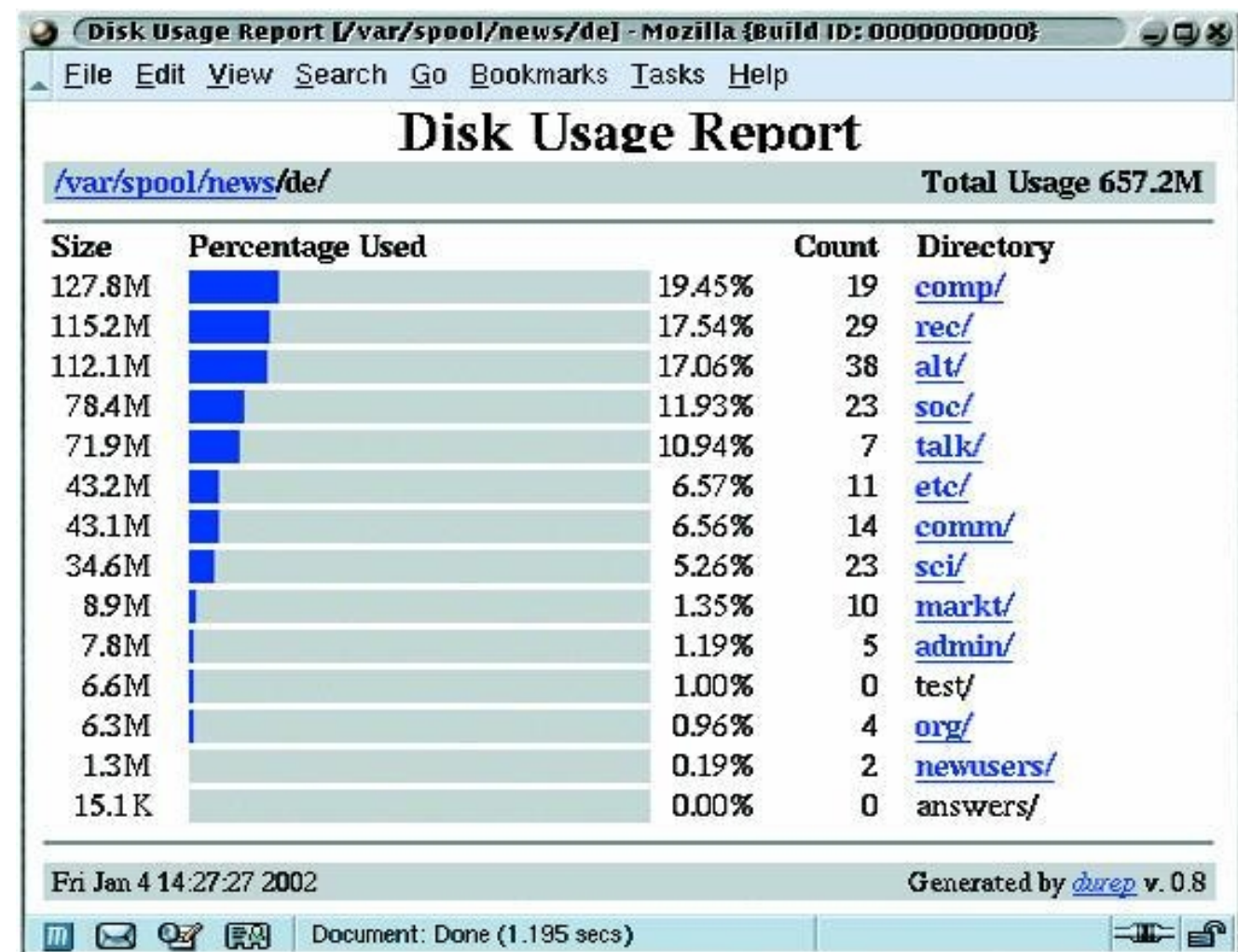
Wie „du“, nur übersichtlich

Verzeichnisgröße auf erster Ebene
akkumuliert:

```
durep -td=1  
/var/spool/news/de/
```

Das gleiche in HTML:

```
durep -w /web/diskusage/  
/var/spool/news/de/
```



Iwatch und Lscyncd

Reagieren auf Inotify-Events

- beide haben ähnlichen Funktionsumfang
- Primärzweck: synchronisieren von Verzeichnissen (lokal/rsync)
- Einschränkung auf bestimmte Events möglich
- rekursives Synchronisieren

Aber auch beliebige andere Aktionen können ausgelöst werden:

- Mail an Admin bei Änderung in einem kritischen Pfad
- Dienste neustarten
- ...

Der Werkzeugkasten

Kommunales Rechenzentrum Niederrhein (KRZN)
Friedrich-Heinrich-Allee 130
47475 Kamp-Lintfort
Internet: www.krzn.de

Vortrag: Charly Kühnast

Danke für's Zuhören!

Fragen? Fragen!

