» KOMMUNALE IT - VON MENSCH ZU MENSCH «

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
```

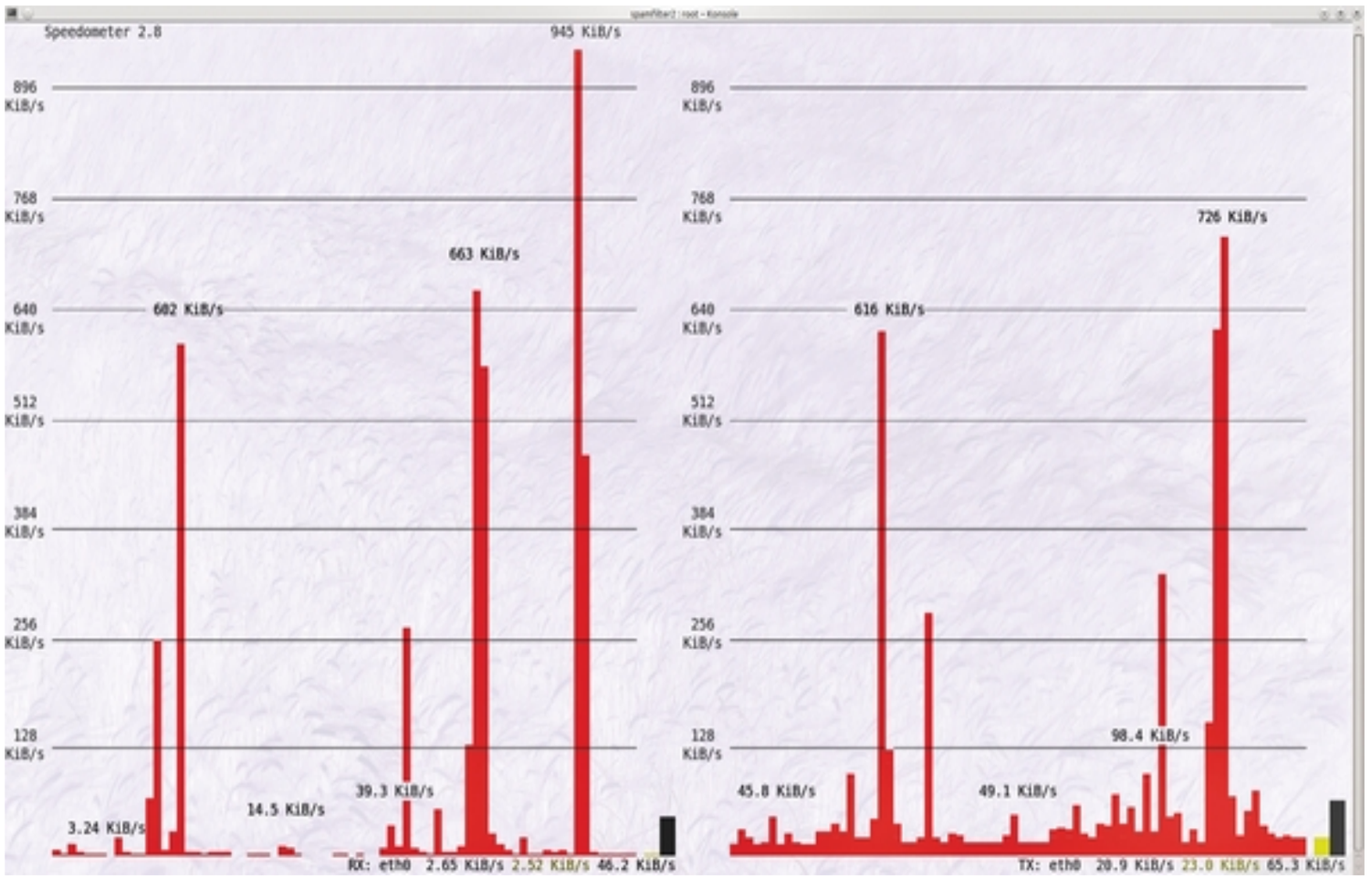
Speedometer

Speedometer zeigt den aktuellen Netzdurchsatz auf der Konsole an.

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

-c = columns

-l = linear (default: logar.)

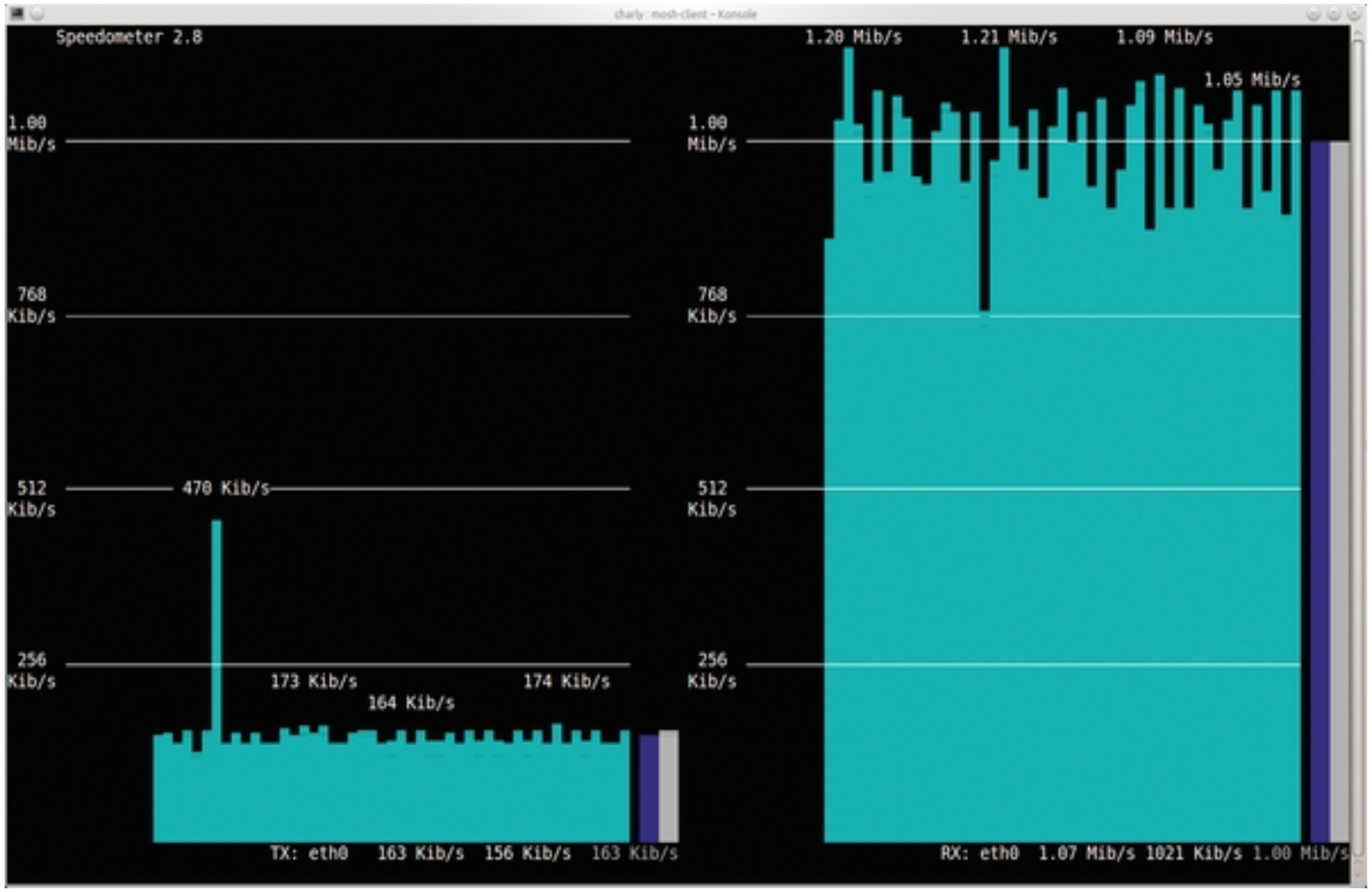


Trickle

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

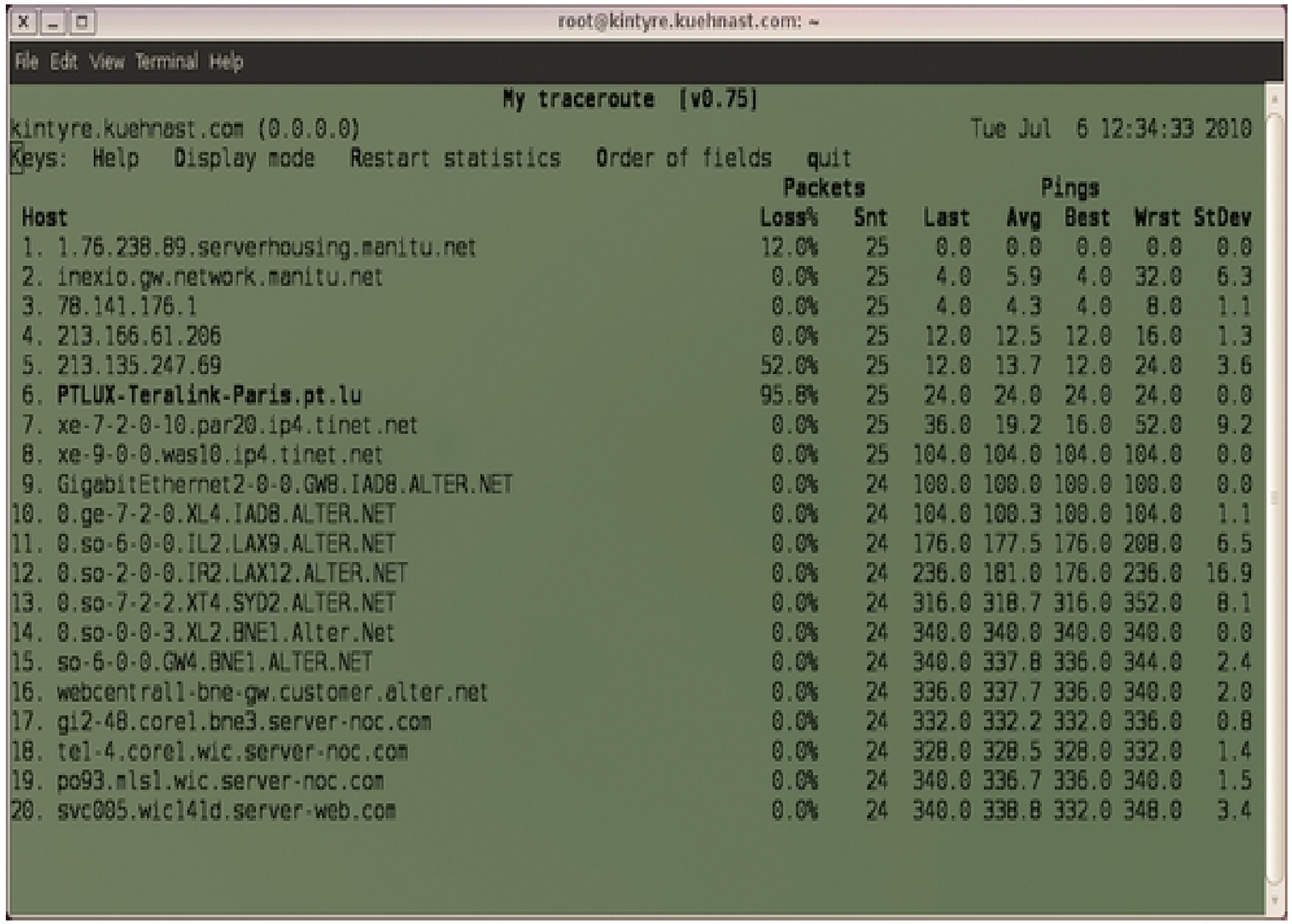


MTR

MTR ist wie traceroute, nur besser.

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

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



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 Verbidungen zu example.com anzeigen:

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

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

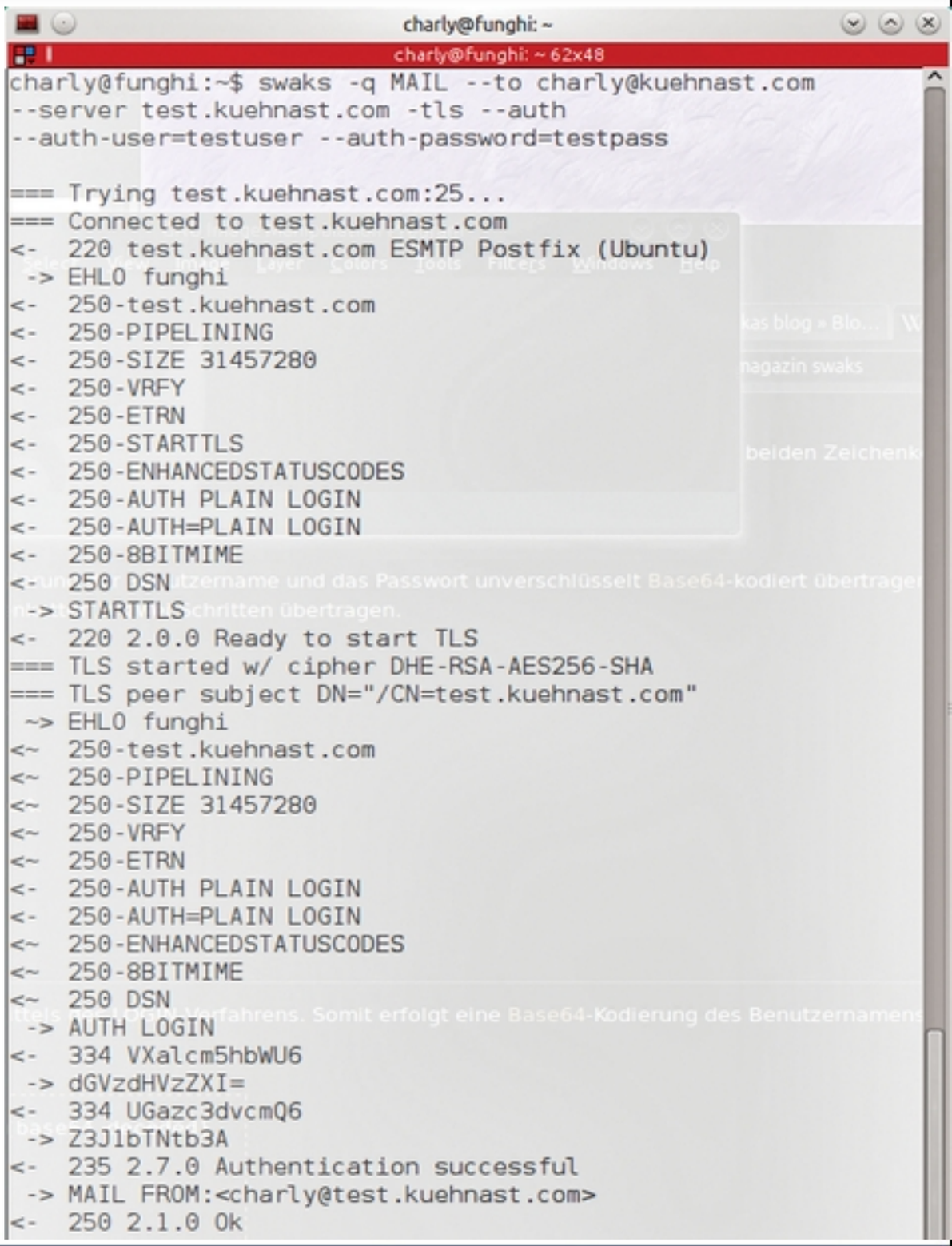
```
lsof -a -u charly -i@example.com:22
```

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



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!

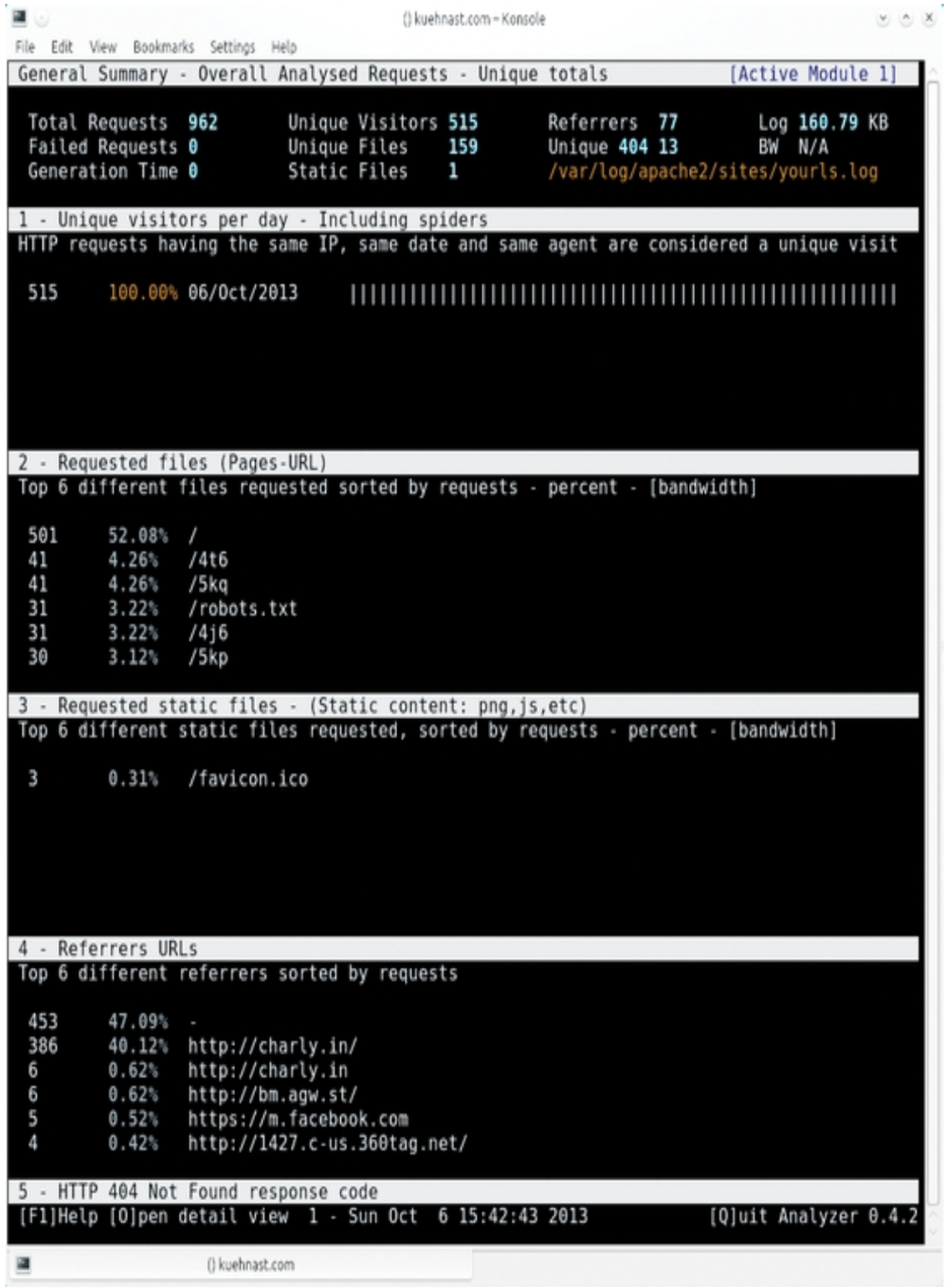
Speak your mind!

GoAccess: Logmittel

GoAccess analysiert Webserver-Logfiles in Echtzeit.

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

„-e <IP>“ = ignore



Smap

Nmap für VoIP

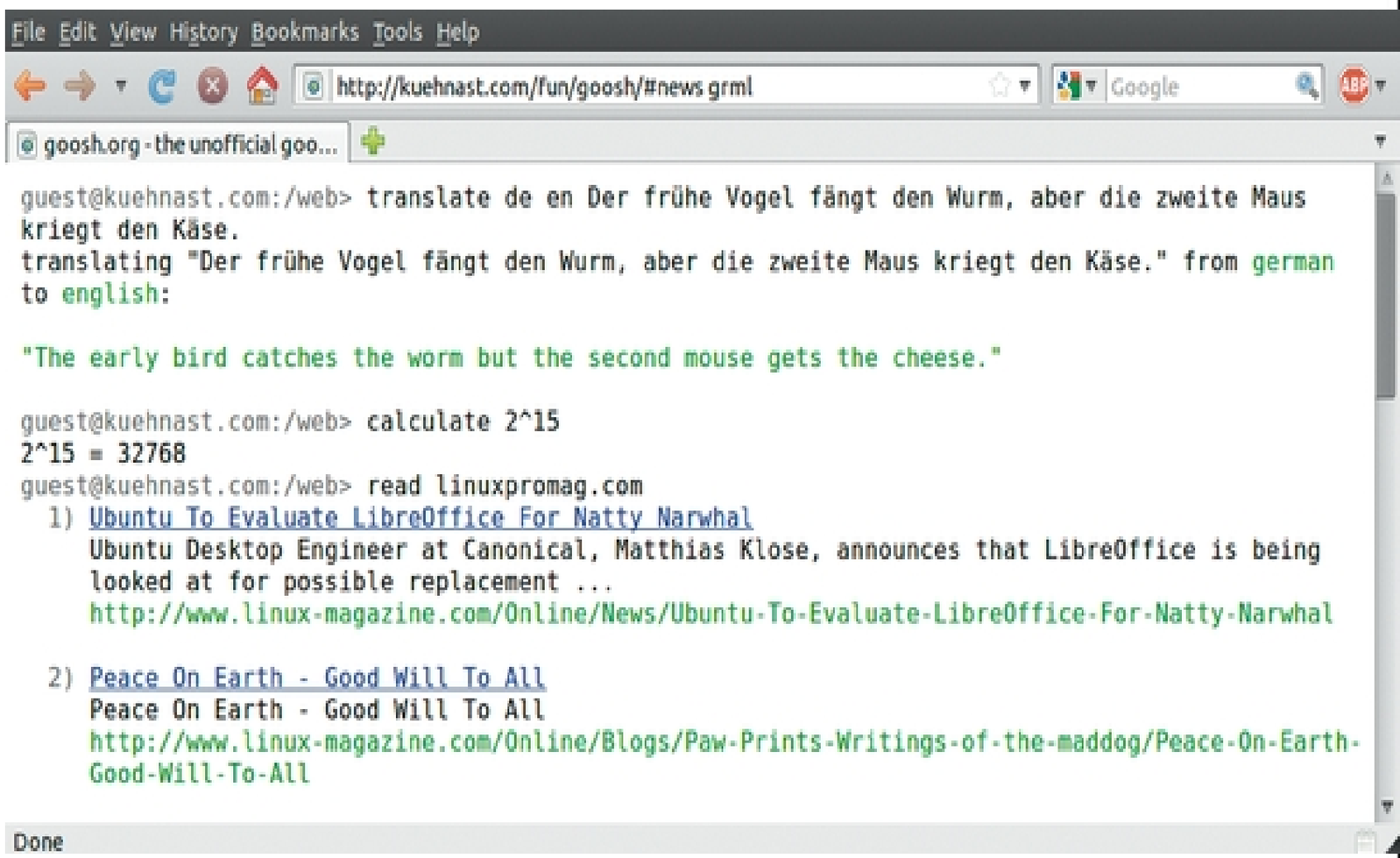
- findet VoIP-Devices im LAN
- Syntax ähnlich Nmap
- Fingerprinting
- Lernmodus

```
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

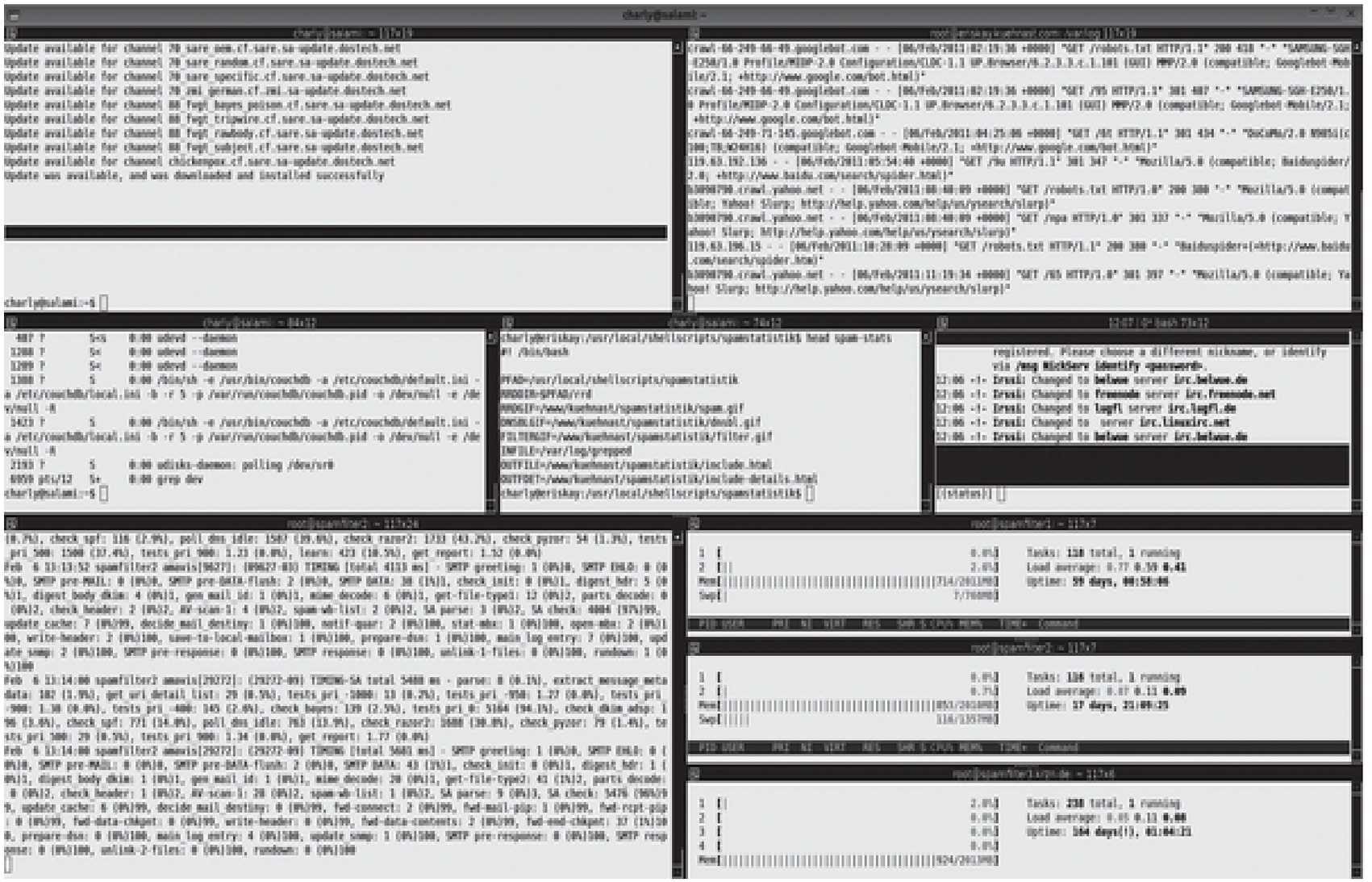
- Textmode-Google
- Shortcuts zu Bilder-, Blog, Wiki-Suche uvm
- Google Translator
- RSS



Terminator

Terminator ist ~~ein Film~~ ein Konsolenmultiplexer für grafische Oberflächen

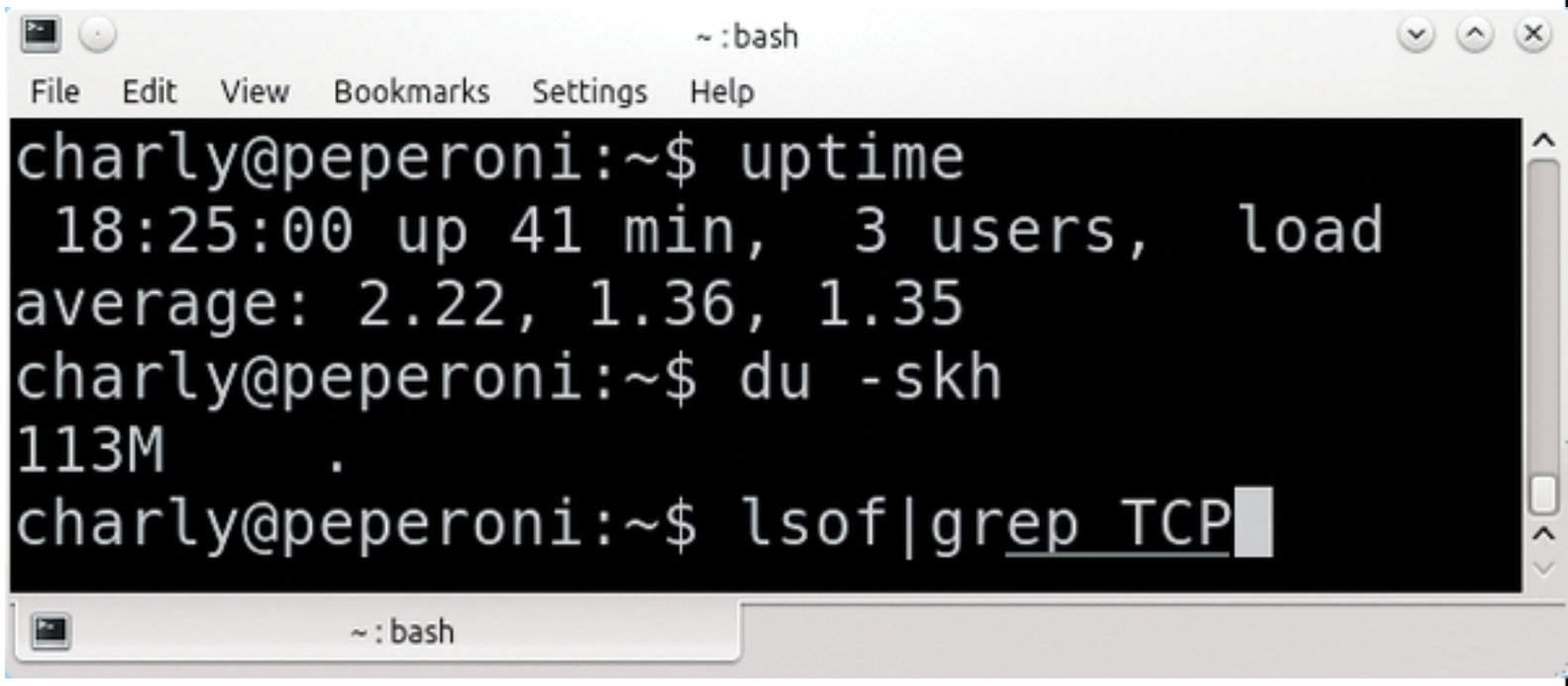
- Einfache Tastaturkommandos
- „Zoomen“
- Drag to reorder
- Vollbildmodus
- Cooler Name



Mosh

Mosh ist ein SSH-Ersatz für schlechte Verbindungsqualität

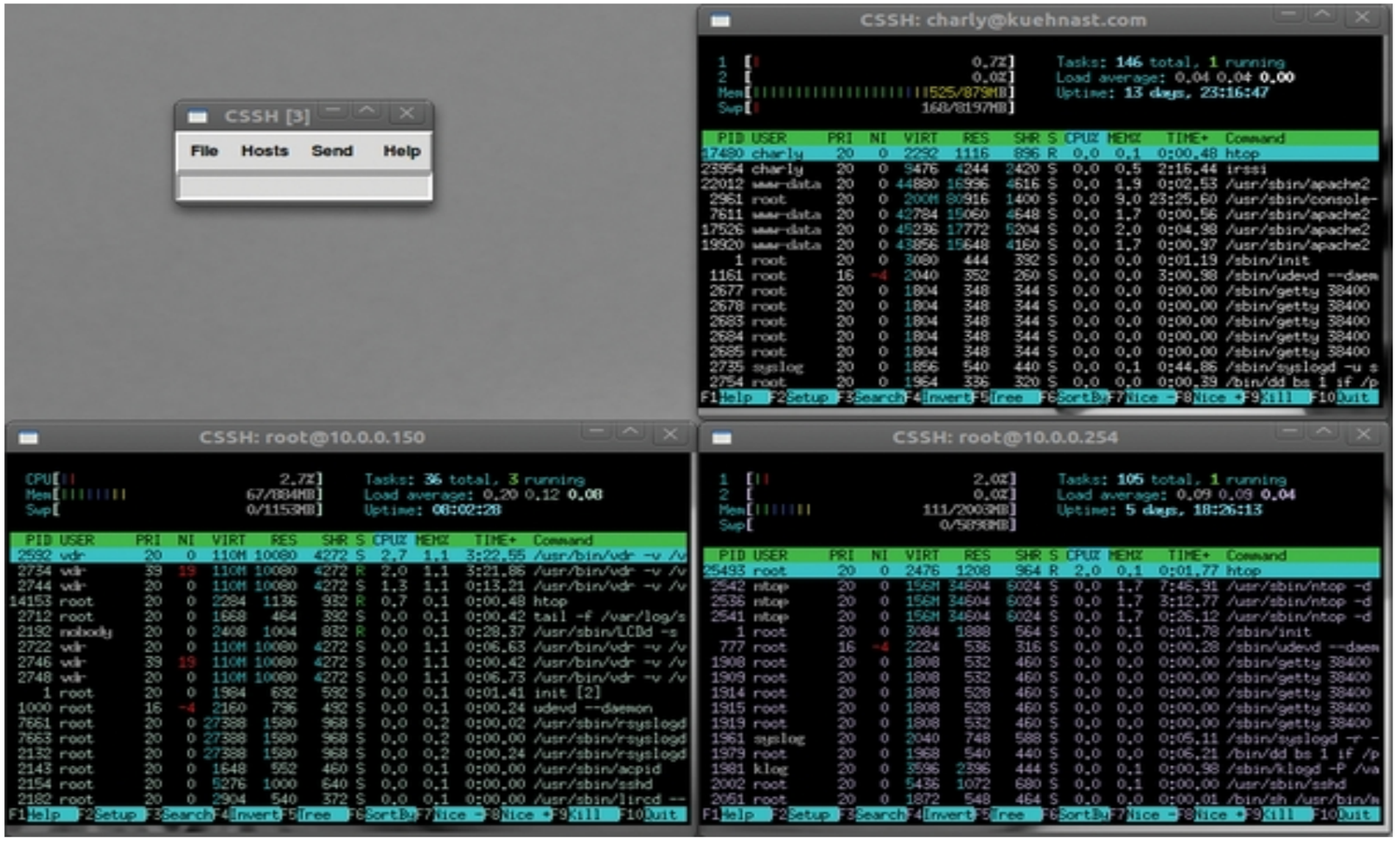
- Verbindungsaufbau über TCP, danach UDP
- Verbindungen sind extrem langlebig und überstehen sogar Wechsel der Client-IP und Reisen mit der Deutschen Bahn



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

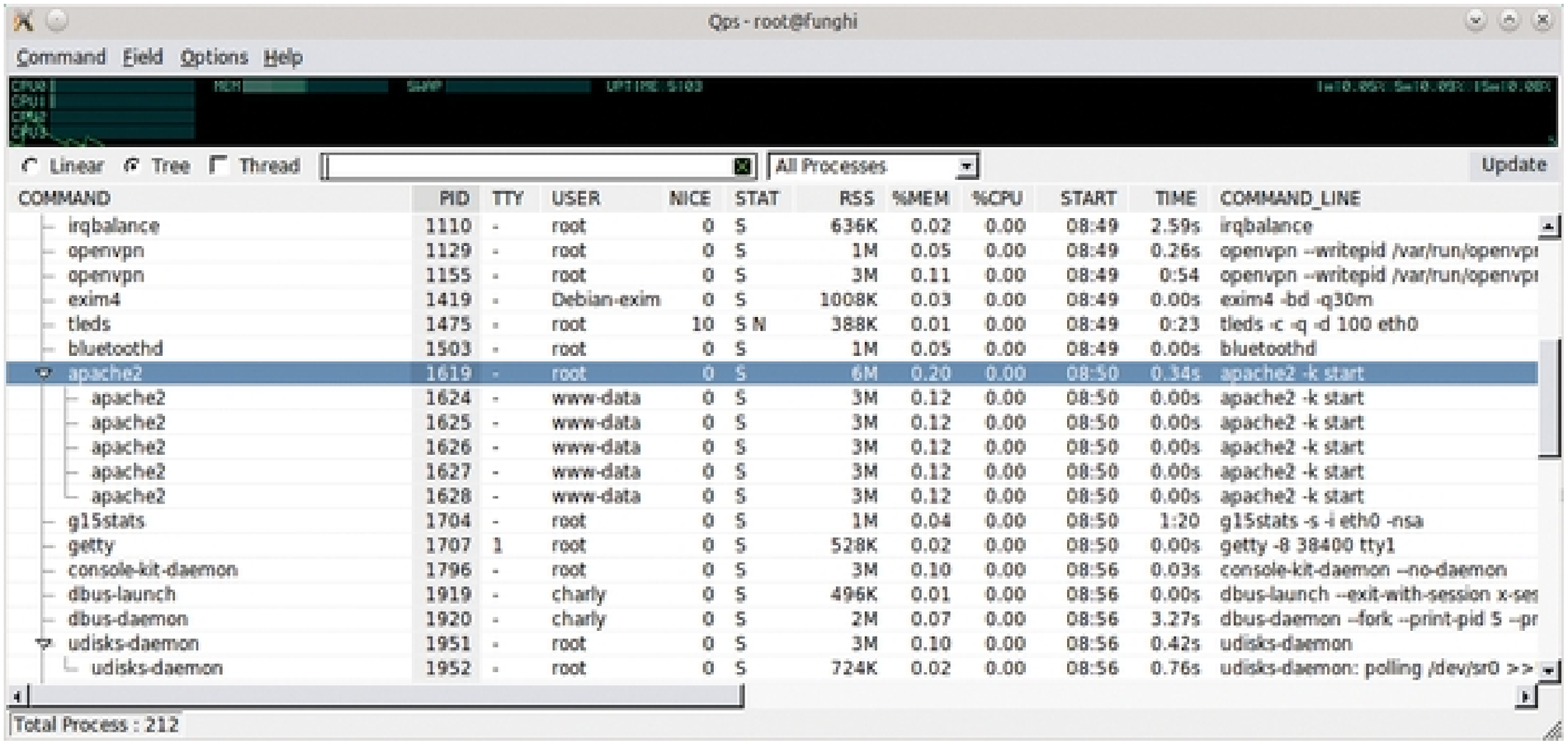
```
tre-agrep -2
<wort> <file>
```

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

Ideal zum Aufspüren von Tippfehlern in Logs

QPS

QPS ist ps, top und lsof in einem grafischen Tool



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:

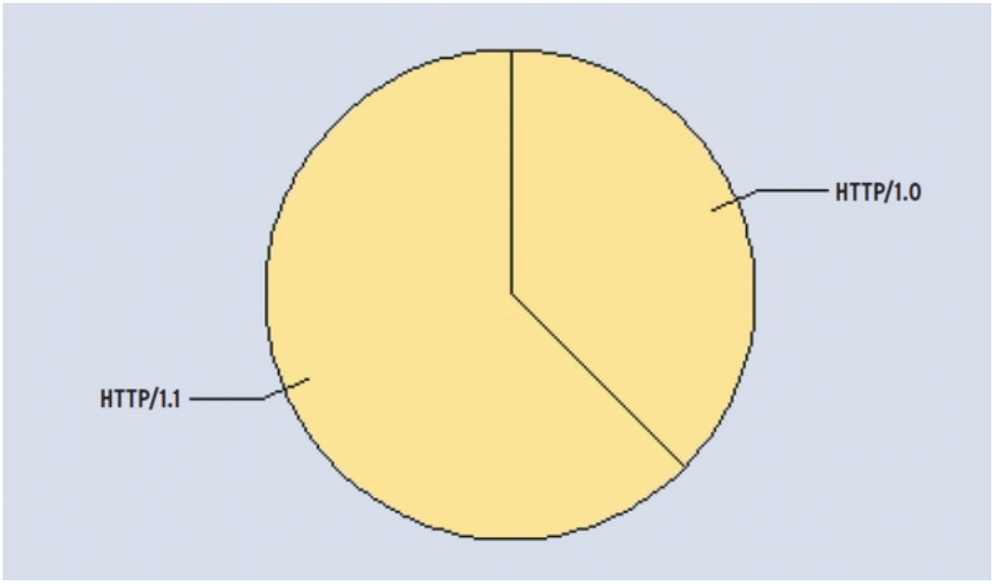
```
MAX_CONNECTIONS=500
PORT=80
BACKEND=2
SERVER1=10.0.0.51:80
SERVER2=10.0.0.52:80
```

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

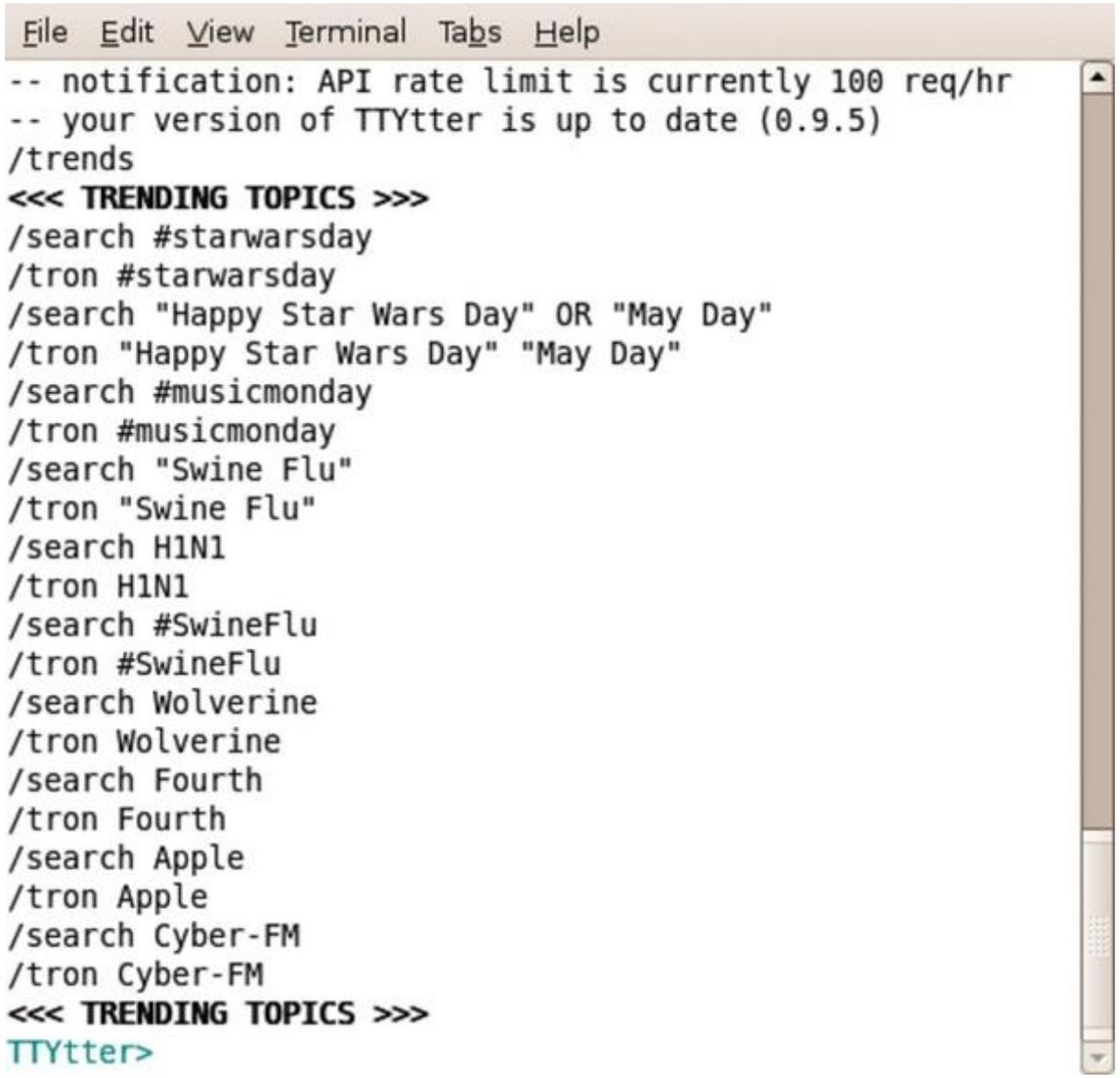
Nichtgrafischer Twitter-Client

Ttytter starten:

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

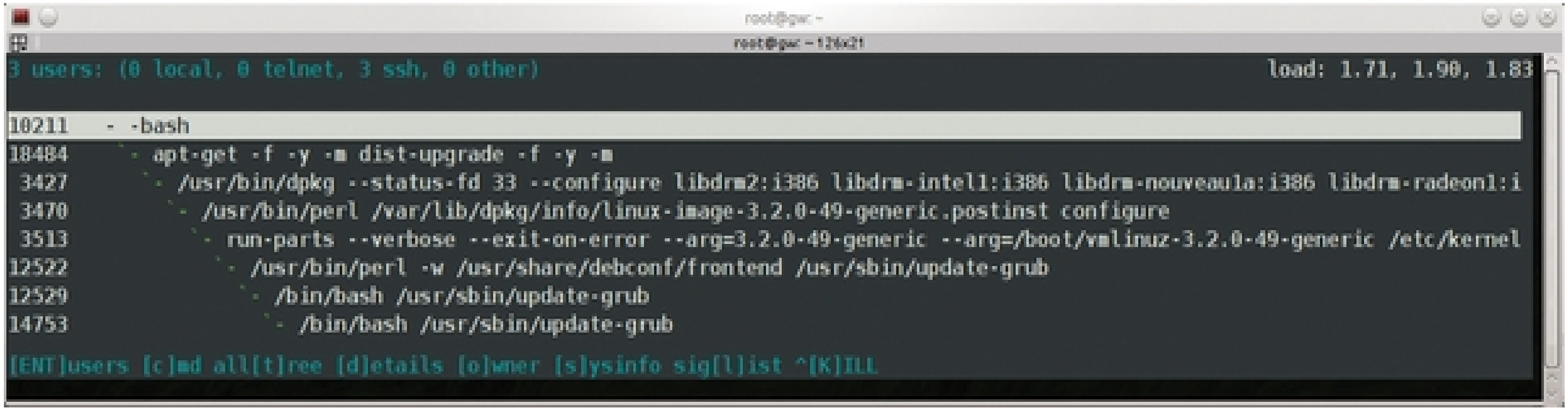
Tweets direkt über die Twitter-API absetzen:

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



Whowatch

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



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

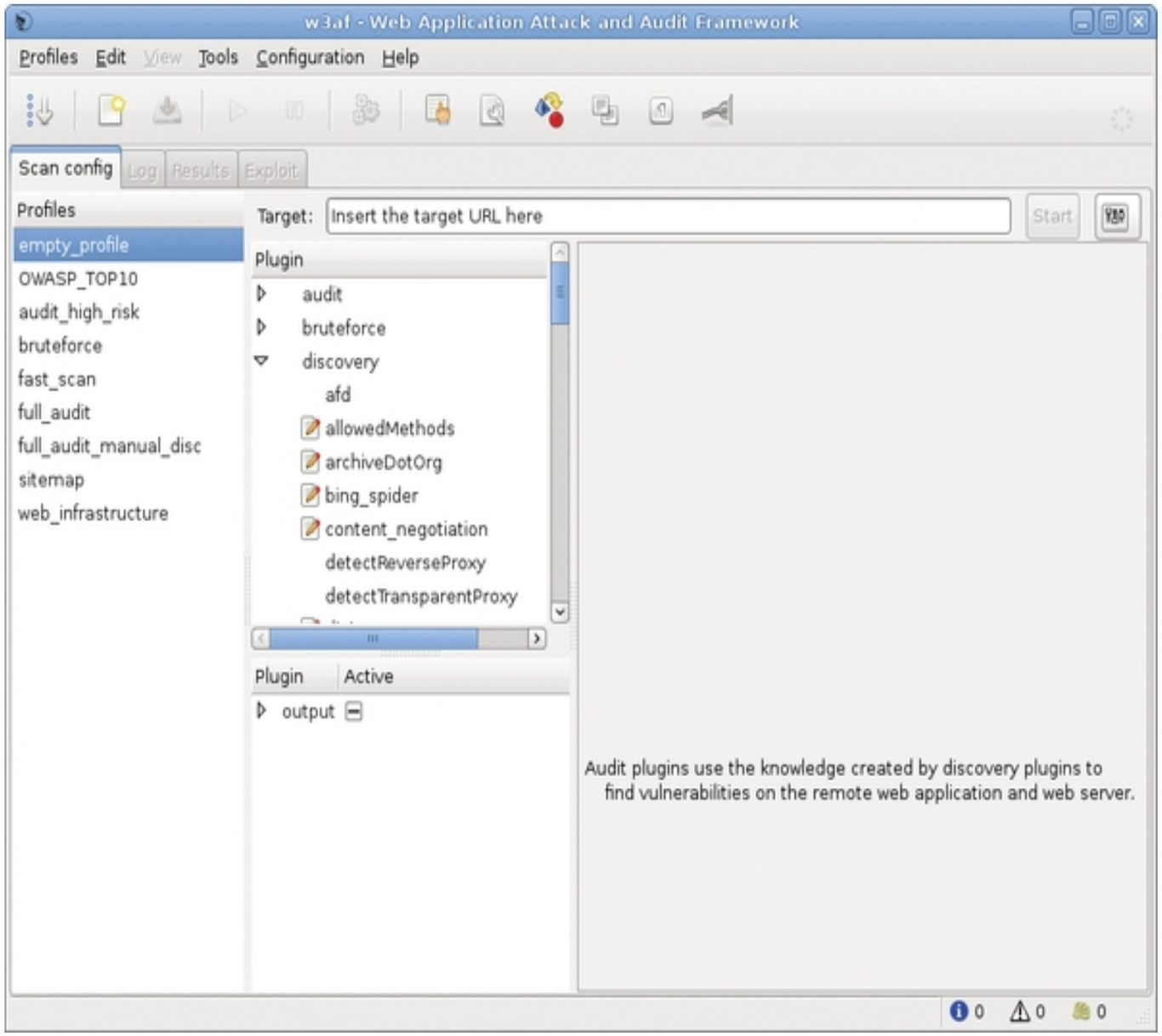
W3AF

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 :

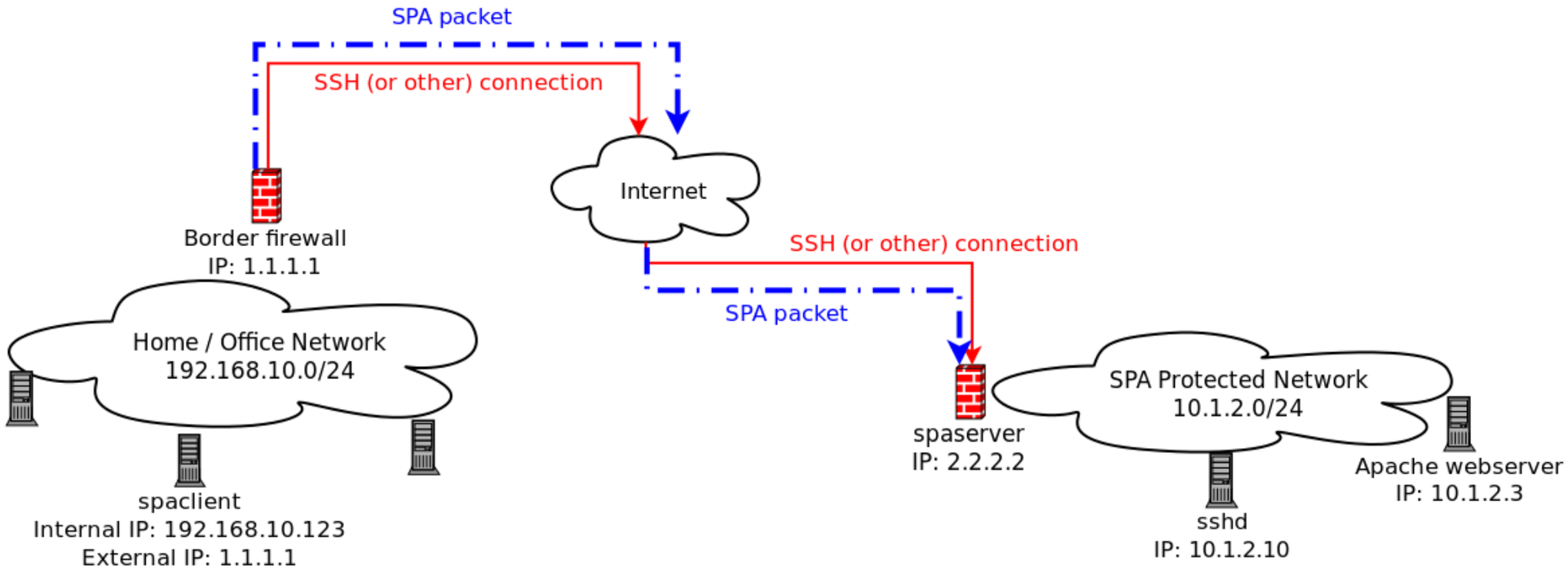
+3HEg,_51P.A@=2U@||{}9Cy

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 EpoohohY aichieFa quephahT Ezoohieh Reicielu febiKies jowooZie
AeBainge oaXooDah Wachiung raiNiupo quiceiVi Leixieki teeZahle siuGhoze
ulieViep eiPhiega tohoShoh eerimaoM feQuicha ieVumoey quookoeX ooYaevae
Ahyohsee quaiShix Aecaebai 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 IWoojeib Ohxongae
laibaiRi oBohquan Oteerohn OnguReez Aogheeph Uaturoig Woeghaej voongohT
charly@salami:~$
```

Single Packet Authentication mit Fwknop

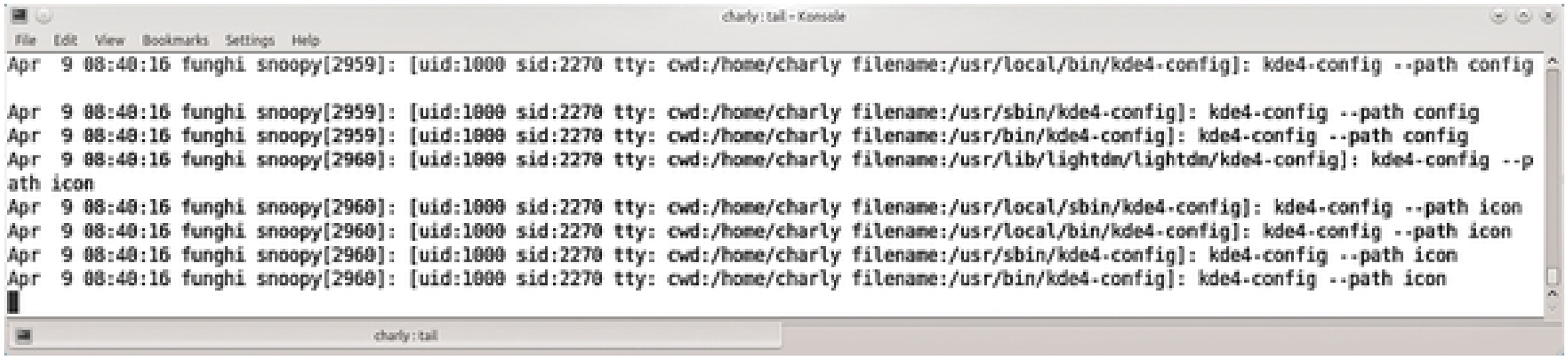
Die bessere Alternative zu Port Knocking



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

Snoopy

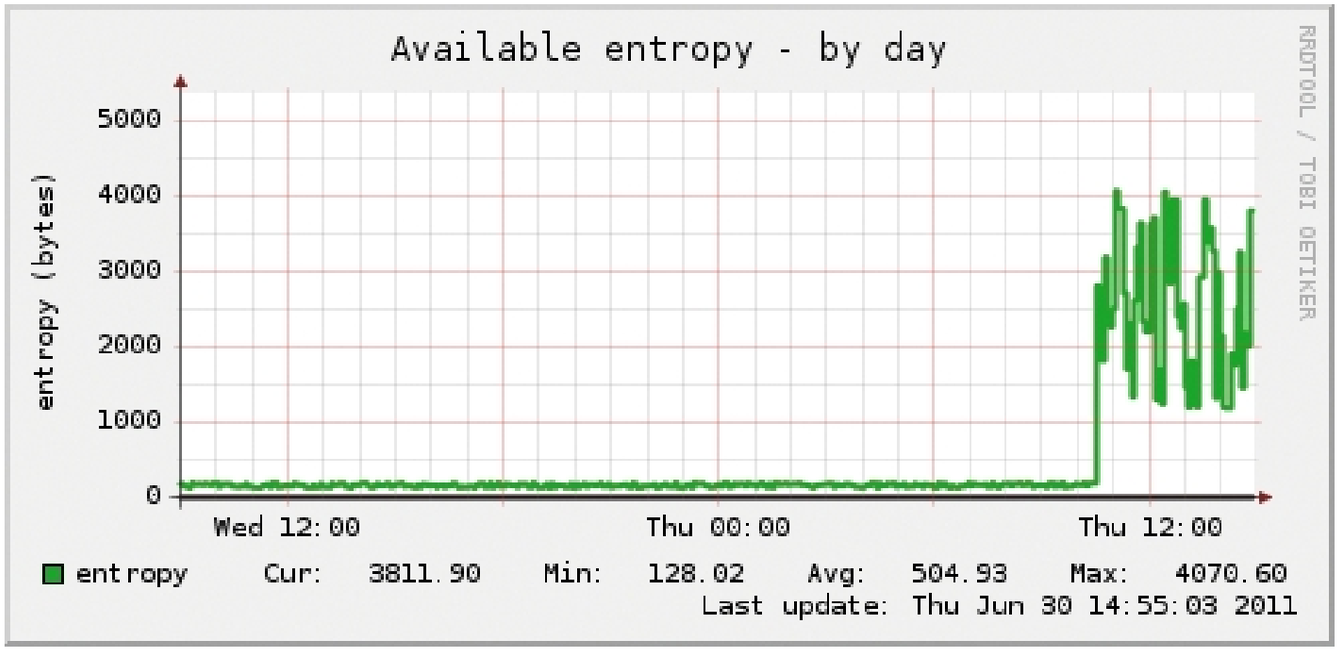
Gedächtnisstütze, Ergänzung zur Bash-History



- 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

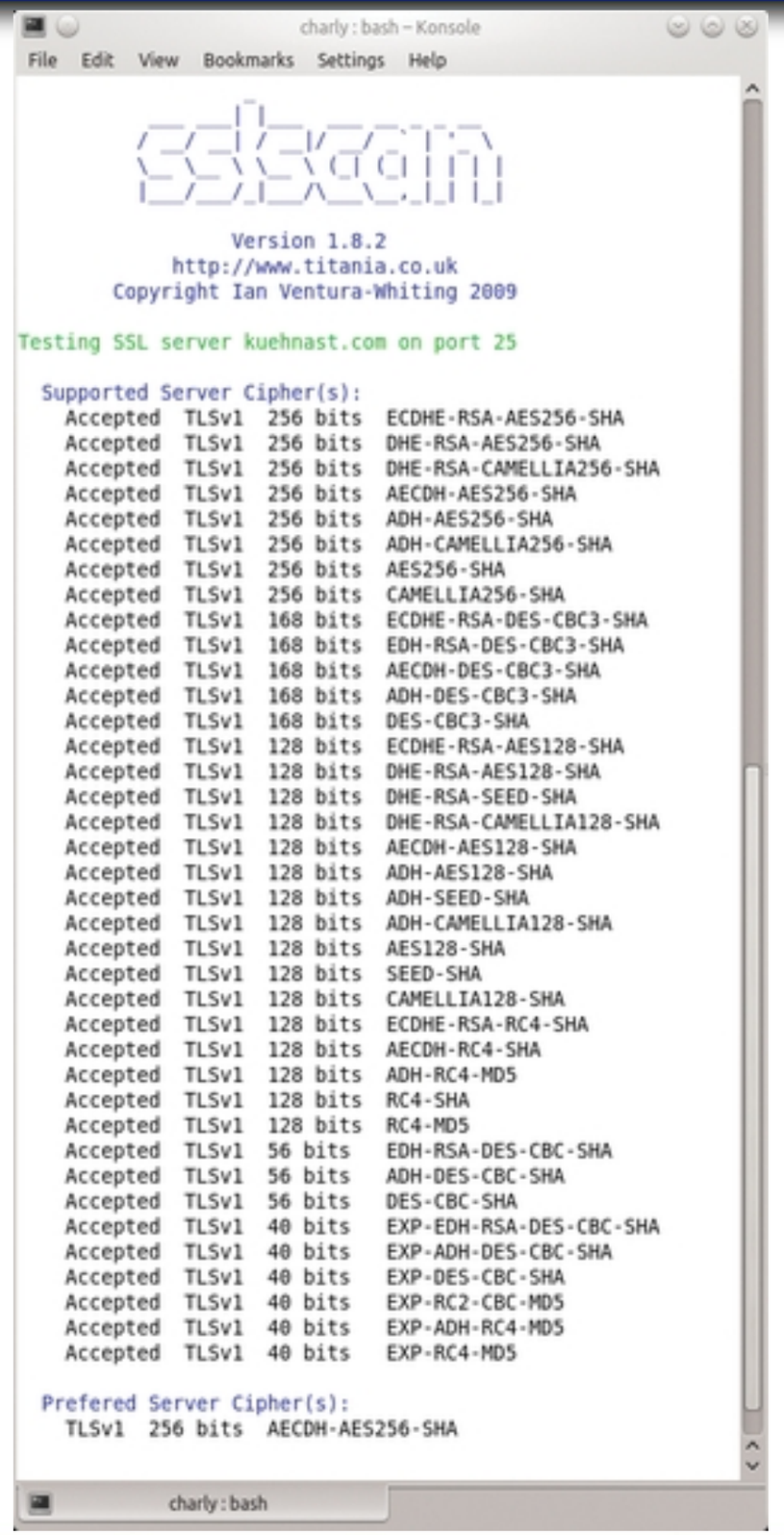
Findet heraus, welche Ciphers ein Server unterstützt (HTTPS und SMTP)

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
```



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

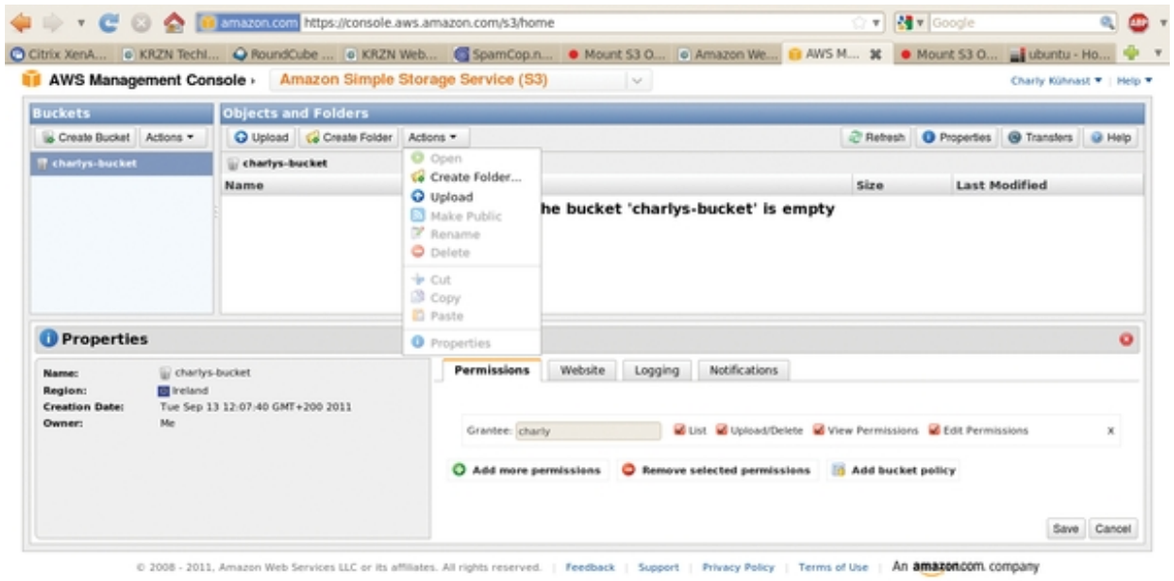
File Edit View Terminal Help

```
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 Parameterhölle).

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

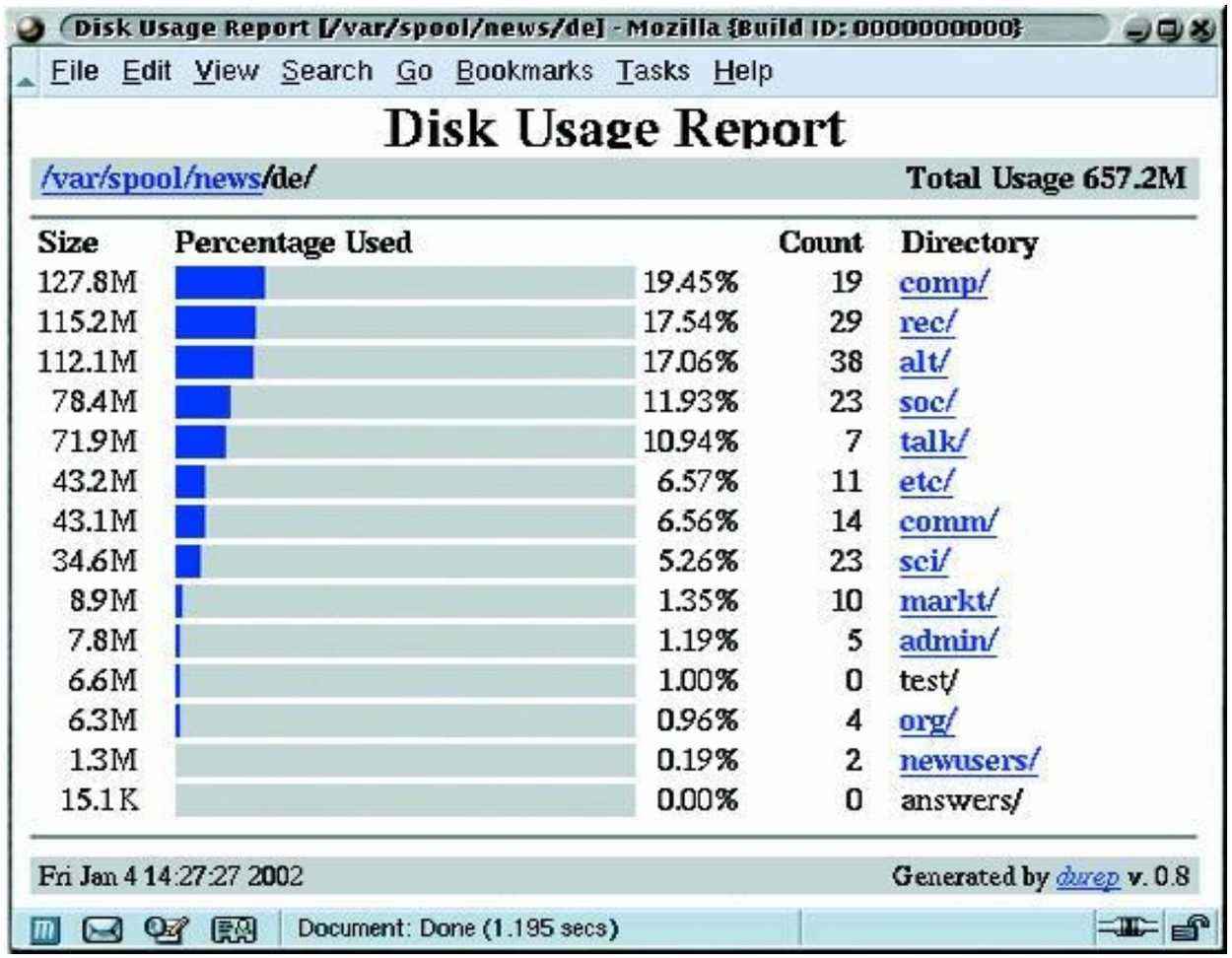
Wie „du“, nur übersichtlich

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!