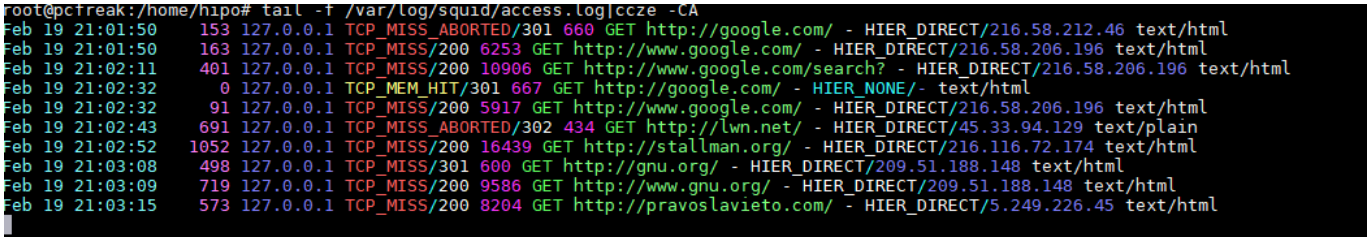
Squid Proxy log timestamp human readable / Convert and beautify Proxy unixtime logs in human-readable form howto

Author : admin



If you have installed Squid Cache Proxy recently and you need to watch who is accessing the proxy and what Internet (website is viewed) under **/var/log/squid/access.log /var/log/store.log /var/log/access.log** etc., you will be unpleasently surprised the log's records are logged in a weird human unreadable format called **UTC** as **Squid Proxy server does not store the date / year / hour time information in a human readable format.**

Squid uses the format:
. and you have to be a robot of a kind or a math genious to read it :)

To display Squid Proxy log in a human readable, luckily you can use below one-liner regular expression.

```
cat access.log | perl -p -e 's/^([0-9]*)/"["."localtime($1)."]"/e'
```

If you have to review squid logs multiple times and on a regular basis you can either set some kind of cmd alias in $HOME/.bashrc such as:

```
alias readproxylog='cat access.log | perl -p -e 's/^([0-9]*)/"["."localtime($1)."]"/e'
```

Or for those who prefer beauty install and use a log beatifier / colorizer such as **ccze**

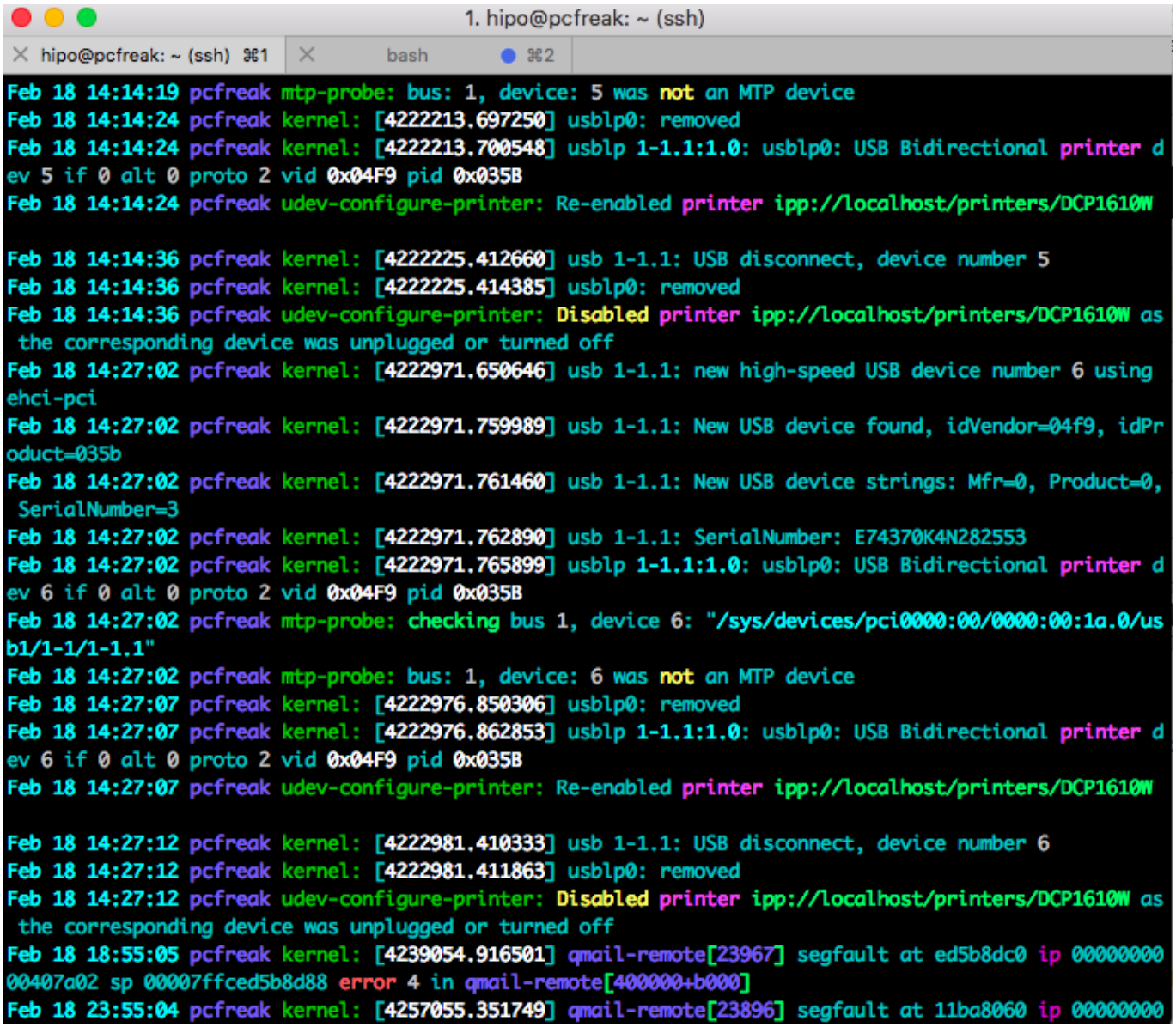
```
root@pcfreak:/home/hipo# apt-cache show ccze|grep -i desc -A 3
Description-en: robust, modular log coloriser
 CCZE is a robust and modular log coloriser, with plugins for apm,
 exim, fetchmail, httpd, postfix, procmail, squid, syslog, ulogd,
 vsftpd, xferlog and more.
Description-md5: 55cd93dbcf614712a4d89cb3489414f6
Homepage: https://github.com/madhouse/ccze
Tag: devel::prettyprint, implemented-in::c, interface::commandline,
 role::program, scope::utility, use::checking, use::filtering,
```

```
root@pcfreak:/home/hipo# apt-get install --yes ccze
```

```
tail -f /var/log/squid/access.loc | ccze -CA
```

ccze is really nice to view /var/log/syslog errors and **make your daily sysadmin life a bit more colorful**

```
tail -f -n 200 /var/log/messages | ccze
```



For a frequent tail + ccze usage with **ccze** you can add to **~/.bashrc following** shell small function

```
tailc () { tail $@ | ccze -A }
```

Below is a list of supported syntax highlighting colorizer:

```
$ ccze -l
Available plugins:

 Name      | Type    | Description
-----------------------------------------------------------
apm        | Partial | Coloriser for APM sub-logs.
distcc     | Full    | Coloriser for distcc(1) logs.
dpkg       | Full    | Coloriser for dpkg logs.
exim       | Full    | Coloriser for exim logs.
fetchmail  | Partial | Coloriser for fetchmail(1) sub-logs.
ftpstats   | Full    | Coloriser for ftpstats (pure-ftpd) logs.
httpd      | Full    | Coloriser for generic HTTPD access and error logs.
icecast    | Full    | Coloriser for Icecast(8) logs.
oops       | Full    | Coloriser for oops proxy logs.
php        | Full    | Coloriser for PHP logs.
postfix    | Partial | Coloriser for postfix(1) sub-logs.
procmail   | Full    | Coloriser for procmail(1) logs.
proftpd    | Full    | Coloriser for proftpd access and auth logs.
squid      | Full    | Coloriser for squid access, store and cache logs.
sulog      | Full    | Coloriser for su(1) logs.
super      | Full    | Coloriser for super(1) logs.
syslog     | Full    | Generic syslog(8) log coloriser.
ulogd      | Partial | Coloriser for ulogd sub-logs.
vsftpd     | Full    | Coloriser for vsftpd(8) logs.
xferlog    | Full    | Generic xferlog coloriser.
```

At many cases for sysadmins like me that prefer clarity over obscurity, even a better solution is to just change in **/etc/squid/squid.conf**
the logging to turn it in human-readable form*, to do so add to config somewhere:*

Logformat squid %tl.%03tu %6tr %>a %Ss/%03Hs %

You will get log output in format like:

18/Feb/2019:18:38:47 +0200.538 4787 y.y.y.y TCP_MISS/200 41841 GET http://google.com/ - DIRECT/x.x.x.x text/html

SQUID's format recognized parameters in above example are as follows:

% a literal % character
>a Client source IP address
>A Client FQDN
>p Client source port
la Local IP address (http_port)
lp Local port number (http_port)
sn Unique sequence number per log line entry
ts Seconds since epoch
tu subsecond time (milliseconds)
tl Local time. Optional strftime format argument
default %d/%b/%Y:%H:%M:%S %z
tg GMT time. Optional strftime format argument
default %d/%b/%Y:%H:%M:%S %z
tr Response time (milliseconds)
dt Total time spent making DNS lookups (milliseconds)