

[wtmp](#), [strings](#), [hostname](#), [ip](#), [egrep](#), [grep](#), [utmpdump](#), [howto](#)

determine connection source hosts

- <http://www.linuxquestions.org/questions/linux-security-4/var-log-wtmp-72976/>
- <https://linux.die.net/man/5/wtmp>

```
strings /var/log/wtmp | egrep -vi "^pts\|^ts\" | grep -P "[0-9_\-]+\.[0-9_\-]+\.[0-9_\-]+\.[0-9_\-]+"
utmpdump /var/log/wtmp | less
/usr/lib/acct/fwtmp < /var/adm/wtmp > /tmp/abc.out
```

From:

<https://wiki.nanoscopic.de/> - nanoscopic wiki

Permanent link:

https://wiki.nanoscopic.de/doku.php/pages/howtos/linuxunix/determine_connection_source_hosts?rev=1638377915

Last update: **2021/12/01 16:58**

