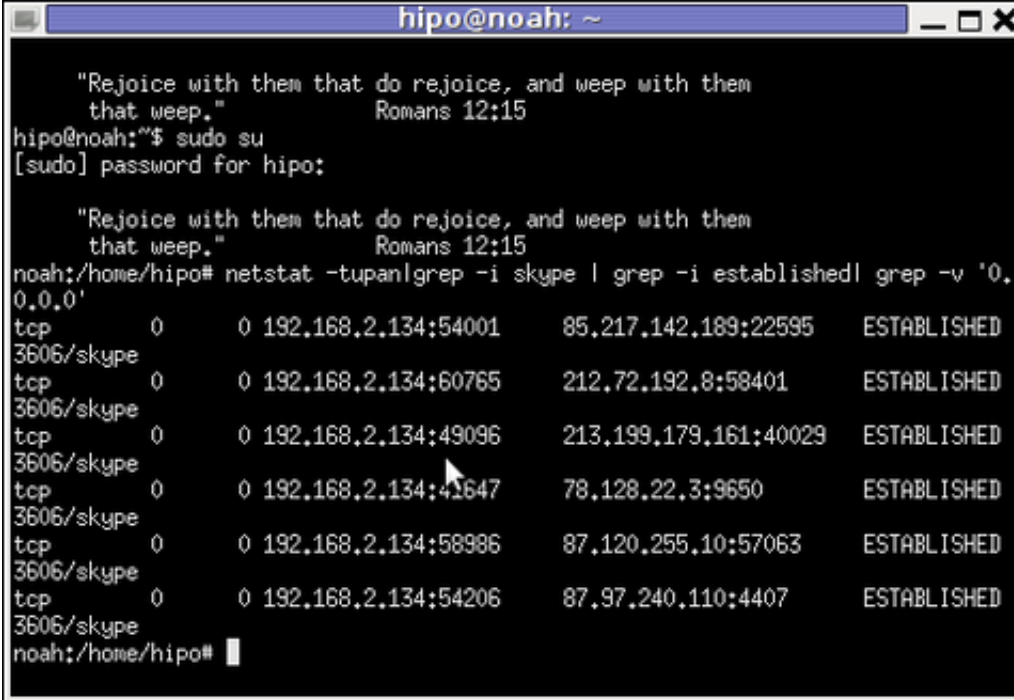


How to check the IP address of Skype (user / Contacts) on GNU / Linux with netstat and whois

Author : admin



```
hipo@noah: ~  
"Rejoice with them that do rejoice, and weep with them  
that weep." Romans 12:15  
hipo@noah:~$ sudo su  
[sudo] password for hipo:  
"Rejoice with them that do rejoice, and weep with them  
that weep." Romans 12:15  
noah:/home/hipo# netstat -tupanl | grep -i skype | grep -i established | grep -v '0.  
0.0.0'  
tcp        0      0 192.168.2.134:54001    85.217.142.189:22595    ESTABLISHED  
3606/skype  
tcp        0      0 192.168.2.134:60765    212.72.192.8:58401     ESTABLISHED  
3606/skype  
tcp        0      0 192.168.2.134:49096    213.199.179.161:40029  ESTABLISHED  
3606/skype  
tcp        0      0 192.168.2.134:41647    78.128.22.3:9650       ESTABLISHED  
3606/skype  
tcp        0      0 192.168.2.134:58986    87.120.255.10:57063    ESTABLISHED  
3606/skype  
tcp        0      0 192.168.2.134:54206    87.97.240.110:4407     ESTABLISHED  
3606/skype  
noah:/home/hipo#
```

Before I explain *how netstat and whois commands can be used to check information about a remote skype user* - e.g. (skype msg is send or received) in **Skype**. I will say in a few words (abstract level), how skype P2P protocol is designed.

Many hard core hackers, certainly know how skype operates, so if this is the case just skip the boring few lines of explanation on *how skype proto works*.

In short **skype transfers its message data as most people know in Peer-to-Peer "mode" (P2P)** - p2p is unique with this that it doesn't require a server to transfer data from one peer to another. Most classical use of p2p networks in the free software realm are the bittorrents.

Skype way of connecting to peer client to other peer client is done via a so called "transport points". To make a P-to-P connection skype goes through a number of middle point destinations. This transport points (peers) are actually other users logged in Skype and the data between point A and point B is transferred via this other logged users in encrypted form. If a skype messages has to be transferred from **Peer A (point A) to Peer B (Point B) or (the other way around)**, the data flows in a way similar to:

$A \rightarrow D \rightarrow F \rightarrow B$

or

$B \rightarrow F \rightarrow D \rightarrow A$

(where D and F are simply other people running skype on their PCs).

The communication from a person A to person B chat in Skype hence, always passes by at least few other IP addresses which are owned by some skype users who happen to be located in the middle geographically between the real geographic location of A (the skype peer sender) and B (The skype peer receiver)..

The exact way skypes communicate is way more complex, this basics however should be enough to grasp the basic skype proto concept for most ppl ...

In order to **find the IP address to a certain skype contact** - one needs to check all *ESTABLISHED* connections of type *skype* protocol with *netsat* within the kernel network stack (connection) queue.

netstat displays few IPs, when skype proto established connections are grepped:

```
noah:~# netstat -tupan|grep -i skype | grep -i established| grep -v '0.0.0.0'
tcp 0 0 192.168.2.134:59677 212.72.192.8:58401 ESTABLISHED 3606/skype
tcp 0 0 192.168.2.134:49096 213.199.179.161:40029 ESTABLISHED 3606/skype
tcp 0 0 192.168.2.134:57896 87.120.255.10:57063 ESTABLISHED 3606/skype
```

Now, as few IPs are displayed, one needs to find out which exactly from the list of the ESTABLISHED IPs is the the Skype Contact from whom are received or to whom are sent the messages in question.

The **blue colored IP address:port** is the local IP address of my host running the Skype client. The **red one is the IP address** of the remote skype host (Skype Name) to which messages are transferred (in the the exact time the netstat command was ran.

The easiest way to find exactly *which, from all the listed IP is the IP address of the remote person* is to *send multiple messages in a low time interval (let's say 10 secs / 10 messages to the remote Skype contact).*

It is a hard task to write 10 msgs for 10 seconds and run 10 times a netstat in separate terminal (simultaneously). Therefore it is a good practice instead of trying your reflex, to run a tiny loop to delay 1 sec its execution and run the prior *netstat* cmd.

To do so open a new terminal window and type:

```
noah:~# for i in $(seq 1 10); do \
sleep 1; echo '-----'; \
netstat -tupan|grep -i skype | grep -i established| grep -v '0.0.0.0'; \
done
-----
tcp 0 0 192.168.2.134:55119 87.126.71.94:26309 ESTABLISHED 3606/skype
-----
```

```
tcp 0 0 192.168.2.134:49096 213.199.179.161:40029 ESTABLISHED 3606/skype
tcp 0 0 192.168.2.134:55119 87.126.71.94:26309 ESTABLISHED 3606/skype
-----
tcp 0 0 192.168.2.134:49096 213.199.179.161:40029 ESTABLISHED 3606/skype
tcp 0 0 192.168.2.134:55119 87.126.71.94:26309 ESTABLISHED 3606/skype
...
```

You see on the first netstat (sequence) exec, there is only 1 IP address to which a skype connection is established, once I sent some new messages to my remote skype friend, another IP immediately appeared. This other IP is actually the IP of the person to whom, I'm sending the "probe" skype messages. Hence, its most likely the skype chat at hand is with a person who has an IP address of the newly appeared **213.199.179.161**

Later to get exact information on who owns *213.199.179.161* and administrative contact info as well as address of the ISP or person owning the IP, do a RIPE **whois**

```
noah:~# whois 213.199.179.161
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to '87.126.0.0 - 87.126.127.255'
inetnum: 87.126.0.0 - 87.126.127.255
netname: BTC-BROADBAND-NET-2
descr: BTC Broadband Service
country: BG
admin-c: LG700-RIPE
tech-c: LG700-RIPE
tech-c: SS4127-RIPE
status: ASSIGNED PA
mnt-by: BT95-ADM
mnt-domains: BT95-ADM
mnt-lower: BT95-ADM
source: RIPE # Filtered
person: Lyubomir Georgiev
.....
```

Note that *this method of finding out the remote Skype Name IP to whom a skype chat is running is not always precise.*

If for instance you tend to chat to many people simultaneously in skype, finding the exact IPs of each of

the multiple Skype contacts will be a very hard not to say impossible task.

Often also by using netstat to capture a Skype Name you're in chat with, there might be plenty of "false positive" IPs..

For instance, Skype might show a remote Skype contact IP correct but still this might not be the IP from which the remote skype user is chatting, as the remote skype side might not have a unique assigned internet IP address but might use his NET connection over a *NAT or DMZ*.

The remote skype user might be hard or impossible to track also if [skype client is run over skype tor proxy for the sake of anonymity](#)

Though it can't be taken as granted that the IP address obtained would be 100% correct with the netstat + whois method, in most cases it is enough to give (at least approximate) info on a **Country and City origin of the person you're skypeing with**.