HOW TO FIND THE IP ADDRESS OF SKYPE USER

I’ve seen this question on several forums around the globe.

Most of the answers were “You can’t”

Strange.

You actually really CAN’T. From Skype :D. But Skype is solely based on P2P connections and you can’t connect to any peer if you don’t have/know his IP address. They simply refuse to disclose their protocol for the public, so we can write our own plugins for Skype.

So, I’ve just had a look at my netstat output (Linux console, sorry – for Windows read below):

```
bash-4.1# netstat -tupan | grep skype

tcp        0      0
0.0.0.0:20530           0.0.0.0:*               LISTEN      2081/skype


tcp        0      0
10.3.71.55:38804        212.75.19.204:6521      ESTABLISHED
2081/skype

tcp        0      0
10.3.71.55:58519        93.152.140.108:23669    ESTABLISHED
2081/skype

udp        0      0
127.0.0.1:59356         0.0.0.0:*                           2081/skype
```

```
udp        0      0
0.0.0.0:20530           0.0.0.0:*                           2081/skype


bash-4.1#
```

And then I've talked to one of my colleagues in office via Skype and rechecked for any new connections:

```
bash-4.1# netstat -tupan | grep skype

tcp        0      0
0.0.0.0:20530           0.0.0.0:*               LISTEN      2081/skype


tcp        0      0
10.3.71.55:38804        212.75.19.204:6521      ESTABLISHED
2081/skype

tcp        0      0
10.3.71.55:58519        93.152.140.108:23669    ESTABLISHED
2081/skype

tcp        0    272
10.3.71.55:55886        10.3.71.97:16592        ESTABLISHED 2081/skype
udp        0      0
127.0.0.1:59356         0.0.0.0:*                           2081/skype

udp        0      0
0.0.0.0:20530           0.0.0.0:*                           2081/skype

bash-4.1#
```

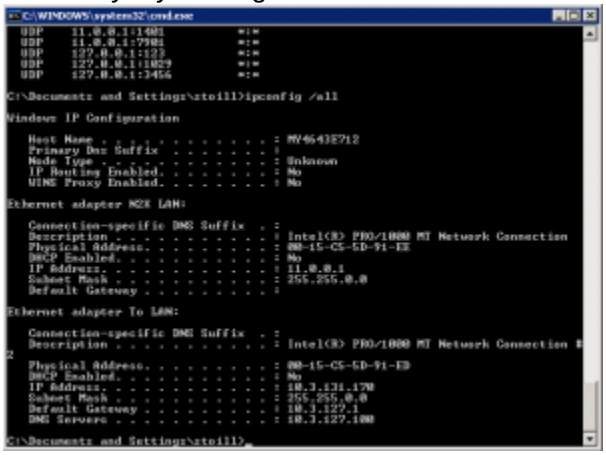
See the red line? *It will not be red in your output. And if there are too much lines, you may take the output in 2 files and then use diff.*

```
bash-4.1# netstat -tupan | grep skype > file1.txt

bash-4.1# netstat -tupan | grep skype > file2.txt

bash-4.1# diff file1.txt file2.txt
```

Than I checked my own IP address:

```
bash-4.1# ifconfig | grep "addr:"

 inet addr:10.3.71.55  Bcast:10.3.255.255  Mask:255.255.0.0 <--------
 inet6 addr: fe80::201:6cff:fe27:4bba/64 Scope:Link
 inet addr:8.0.0.2  Bcast:8.0.255.255  Mask:255.255.0.0
 inet addr:9.0.0.2  Bcast:9.0.255.255  Mask:255.255.0.0
 inet addr:10.0.0.2  Bcast:10.0.255.255  Mask:255.255.0.0
 inet addr:127.0.0.1  Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
bash-4.1#
```

Obviously my colleague's IP address is 10.3.71.97.



It's as easy as this in Windows actually. You only need to enter the Command prompt (Start -> Run -

> cmd) and enter netstat the same way as with Linux (don't know about the options after the dash and you will not have grep and protocol resolution). The Skype connection port is varying every time, so you may be in a bit of an analyze, but basically it's the same. Your own IP address can be seen if you enter the command **ipconfig /all**:
If you are really LOST in CMD mode. Try this little nifty program from Windows SysInternals. It's doing it's job splendidly. Just don't forget to use the sort and filter functions if you happen to have too much connections with your PC. The principle is the same.
That's basically all. Remember your IP address (see above) Talk in Skype to the person for which IP address you are interested and watch the new connection Skype opens. Voila. The IP address is there.

All of this will not happen if the person in you are interested is using Proxy or any anonymizer software. Then you will see random Proxy address. And to try to hack a proxy server is not something that you will just find out by reading blogs and forums. Also, there is some chance that Microsoft will change part of the Skype protocol. Good luck. 
There are a lot of attempts to crack Skype protocol, all of them in vain. Perhaps some day the protocol will be reverse engineered and Skype security will not be so tight. There are rumors of ONE person who did this and got a nifty $um of money for his silence.

Anyway. Feel free to bridge your Skype connection over a sniffer and try your luck. I cannot teach you how to disassemble the Skype protocol.

Source : http://www.m0rd0r.eu/category/l2/page/2/