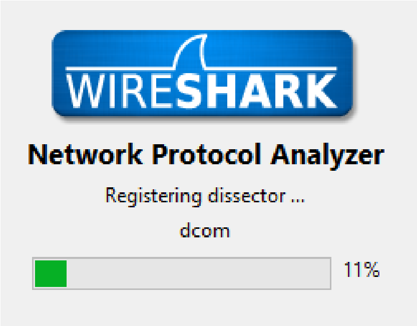
How to get somebody’s IP on Skype or Steam using Wireshark

A simple Tutorial by Xaotic

1. Setup

Download Wireshark https://www.wireshark.org/download.html

Open it. The start up should look like this.



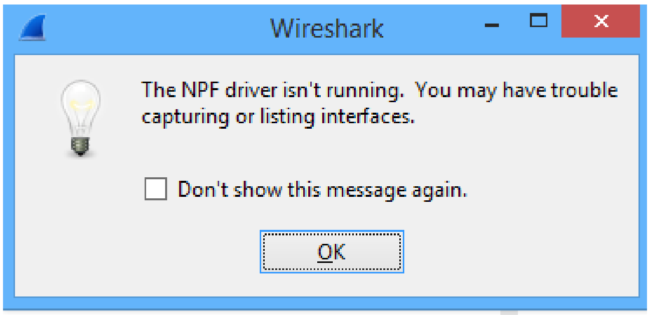
Network Protocol Analyzer

Registering dissector ...

dcom

11%

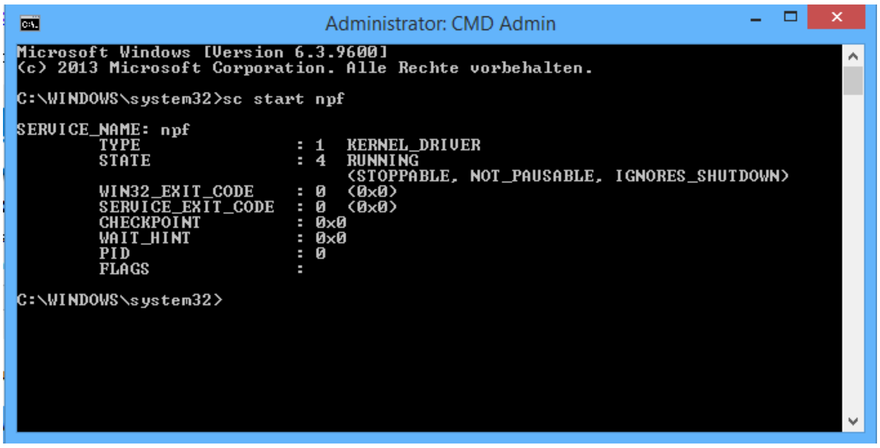
As soon as it started up you might see the following message.



The NPF driver isn't running. You may have trouble capturing or listing interfaces.

☐ Don't show this message again.

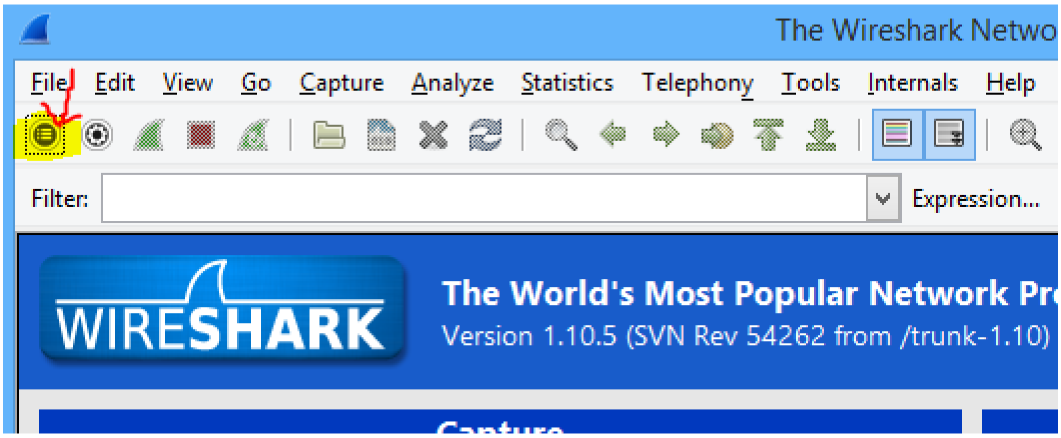
In this case start cmd.exe as Administrator and enter **“sc start npf”** (without “)



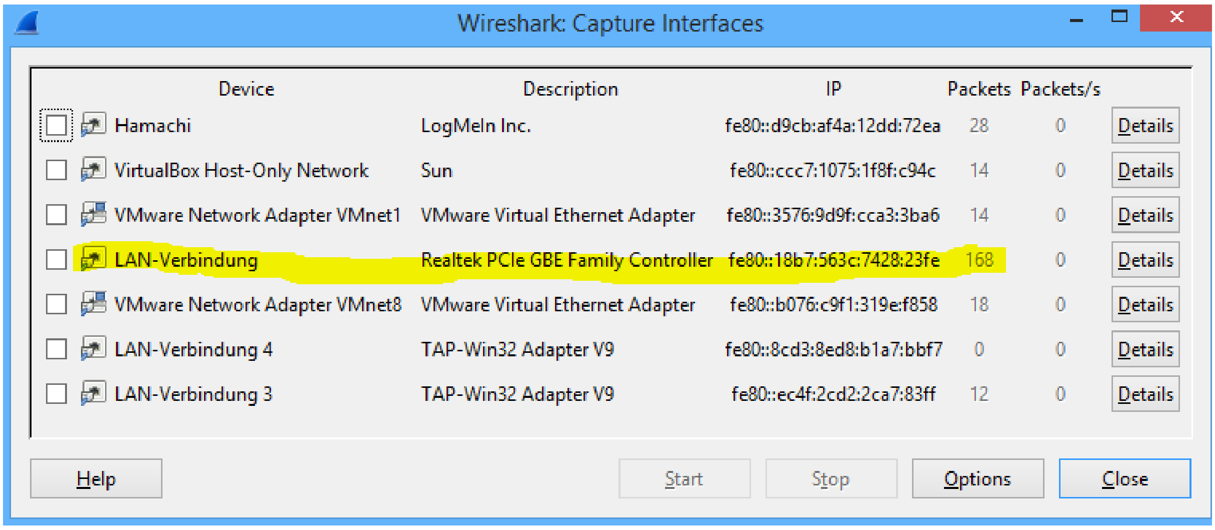
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>sc start npf

SERVICE_NAME: npf
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 0
        FLAGS              :

C:\WINDOWS\system32>
```

After that is done restart it.

To select an interface to capture click this button right here.


The Wireshark Netwo
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
WIRESHARK
The World's Most Popular Network Pr
Version 1.10.5 (SVN Rev 54262 from /trunk-1.10)
Capture

You see a window popping up. Wait a couple seconds and take a look at which interface you receive the most packets.


Wireshark: Capture Interfaces

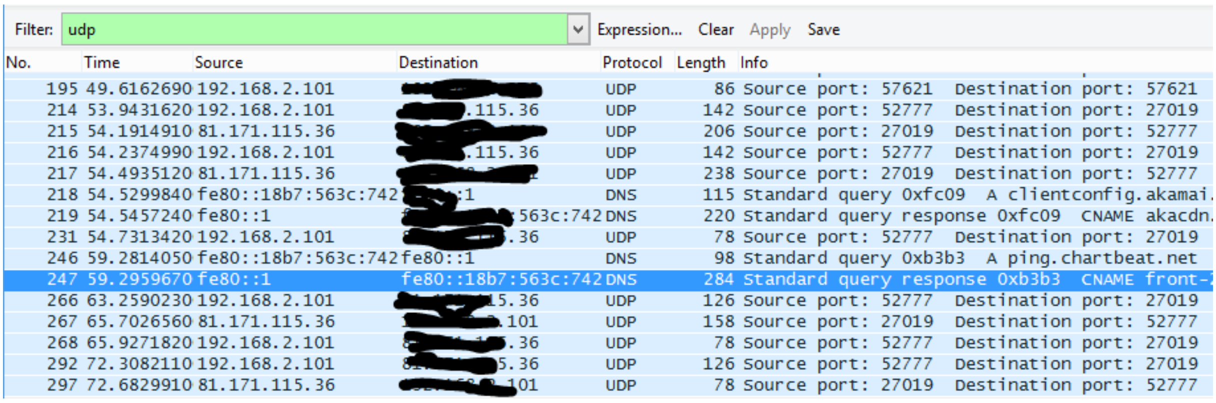
	Device	Description	IP	Packets	Packets/s	
□	Hamachi	LogMeIn Inc.	fe80::d9cb:af4a:12dd:72ea	28	0	Details
□	VirtualBox Host-Only Network	Sun	fe80::ccc7:1075:1f8f:c94c	14	0	Details
□	VMware Network Adapter VMnet1	VMware Virtual Ethernet Adapter	fe80::3576:9d9f:cca3:3ba6	14	0	Details
□	LAN-Verbindung	Realtek PCIe GBE Family Controller	fe80::18b7:563c:7428:23fe	168	0	Details
□	VMware Network Adapter VMnet8	VMware Virtual Ethernet Adapter	fe80::b076:c9f1:319e:f858	18	0	Details
□	LAN-Verbindung 4	TAP-Win32 Adapter V9	fe80::8cd3:8ed8:b1a7:bbf7	0	0	Details
□	LAN-Verbindung 3	TAP-Win32 Adapter V9	fe80::ec4f:2cd2:2ca7:83ff	12	0	Details

For me it's "LAN-Verbindung" as I am obviously using LAN to connect to the Internet.

Check the checkbox to the left and press Start.

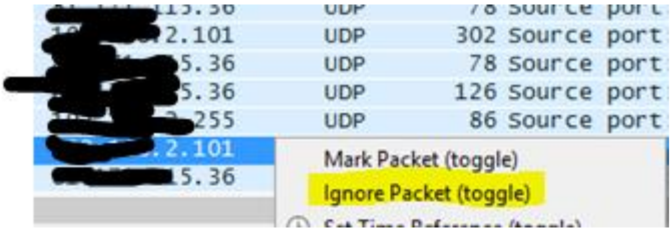
Now you see a lot of packets reaching us. Just a couple of them are interesting.

In "Filter" type "udp". Now you only see UDP packets!


Filter: udp

No.	Time	Source	Destination	Protocol	Length	Info
195	49.6162690	192.168.2.101	[redacted]	UDP	86	Source port: 57621 Destination port: 57621
214	53.9431620	192.168.2.101	[redacted].115.36	UDP	142	Source port: 52777 Destination port: 27019
215	54.1914910	81.171.115.36	[redacted]	UDP	206	Source port: 27019 Destination port: 52777
216	54.2374990	192.168.2.101	[redacted].115.36	UDP	142	Source port: 52777 Destination port: 27019
217	54.4935120	81.171.115.36	[redacted]	UDP	238	Source port: 27019 Destination port: 52777
218	54.5299840	fe80::18b7:563c:742	[redacted]:1	DNS	115	Standard query 0xfc09 A clientconfig.akamai.
219	54.5457240	fe80::1	[redacted]563c:742	DNS	220	Standard query response 0xfc09 CNAME akacdn.
231	54.7313420	192.168.2.101	[redacted].36	UDP	78	Source port: 52777 Destination port: 27019
246	59.2814050	fe80::18b7:563c:742	fe80::1	DNS	98	Standard query 0xb3b3 A ping.chartbeat.net
247	59.2959670	fe80::1	fe80::18b7:563c:742	DNS	284	Standard query response 0xb3b3 CNAME front-
266	63.2590230	192.168.2.101	[redacted]5.36	UDP	126	Source port: 52777 Destination port: 27019
267	65.7026560	81.171.115.36	[redacted].101	UDP	158	Source port: 27019 Destination port: 52777
268	65.9271820	192.168.2.101	[redacted].36	UDP	78	Source port: 52777 Destination port: 27019
292	72.3082110	192.168.2.101	[redacted]5.36	UDP	126	Source port: 52777 Destination port: 27019
297	72.6829910	81.171.115.36	[redacted]01	UDP	78	Source port: 27019 Destination port: 52777

There are most likely still some packets you can see.



```
[redacted]13.36   UDP    78 Source port
[redacted]2.101   UDP   302 Source port
[redacted]5.36    UDP    78 Source port
[redacted]5.36    UDP   126 Source port
[redacted]255     UDP    86 Source port
[redacted]2.101
[redacted]5.36
```

As we don’t need those just wait out a bit look at those who appear frequently and right click them and press Ignore Packet.

*This is optional and does not work out everytime.

2. Getting the targets IP

Now we are done setting up, lets call our victim/target.

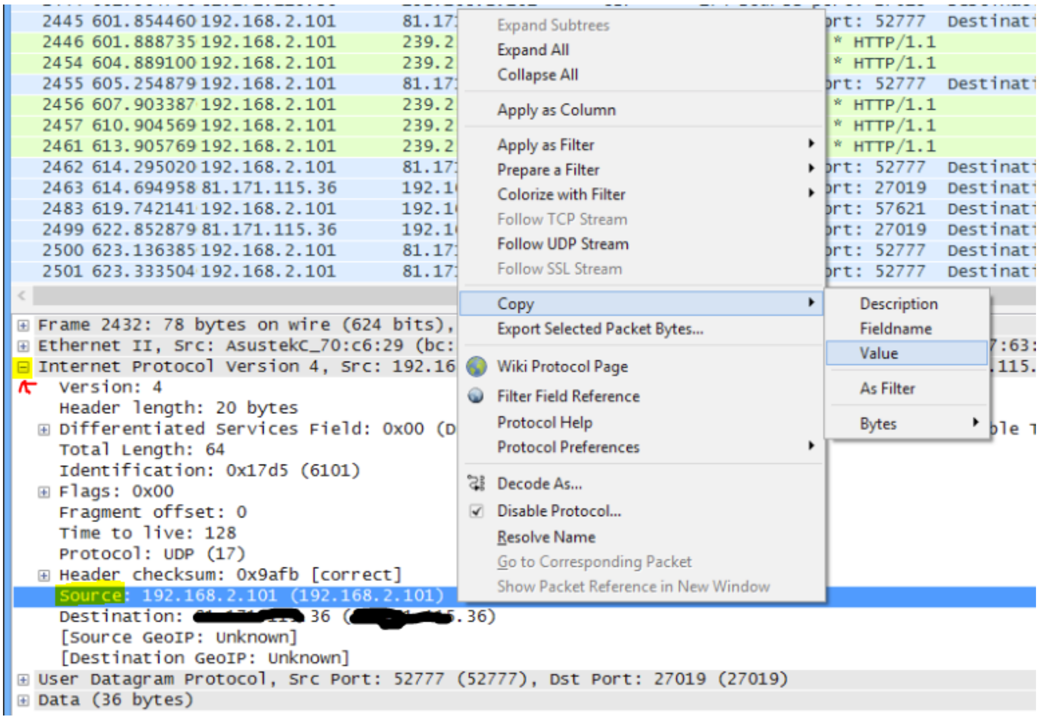
As Skype and Steam is mostly peer to peer you can easily fish out IPs.

As soon as he picks up you got his IP already. Now just gotta find out which it is.

A new IP should appear in Wireshark frequently.

Left click the IP, expand “Internet Protocol (…)” and right click the Source, Copy and then press Value.

You now copied his IP.



```
2445 601.854460 192.168.2.101    81.17    rt: 52777  Destinat
2446 601.888735 192.168.2.101    239.2    * HTTP/1.1
2454 604.889100 192.168.2.101    239.2    * HTTP/1.1
2455 605.254879 192.168.2.101    81.17    rt: 52777  Destinat
2456 607.903387 192.168.2.101    239.2    * HTTP/1.1
2457 610.904569 192.168.2.101    239.2    * HTTP/1.1
2461 613.905769 192.168.2.101    239.2    * HTTP/1.1
2462 614.295020 192.168.2.101    81.17    rt: 52777  Destinat
2463 614.694958 81.171.115.36    192.1    rt: 27019  Destinat
2483 619.742141 192.168.2.101    192.1    rt: 57621  Destinat
2499 622.852879 81.171.115.36    192.1    rt: 27019  Destinat
2500 623.136385 192.168.2.101    81.17    rt: 52777  Destinat
2501 623.333504 192.168.2.101    81.17    rt: 52777  Destinat
```

```
⊞ Frame 2432: 78 bytes on wire (624 bits),
⊞ Ethernet II, Src: AsustekC_70:c6:29 (bc:                    :63:
⊟ Internet Protocol Version 4, Src: 192.16                    115.
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (D                    ble 1
    Total Length: 64
    Identification: 0x17d5 (6101)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x9afb [correct]
    Source: 192.168.2.101 (192.168.2.101)
    Destination: [redacted]36 ([redacted].36)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ User Datagram Protocol, Src Port: 52777 (52777), Dst Port: 27019 (27019)
⊞ Data (36 bytes)
```

*Source is my IPv4 Address because I just used a random packet as no contact was willing to help me ☹ lel

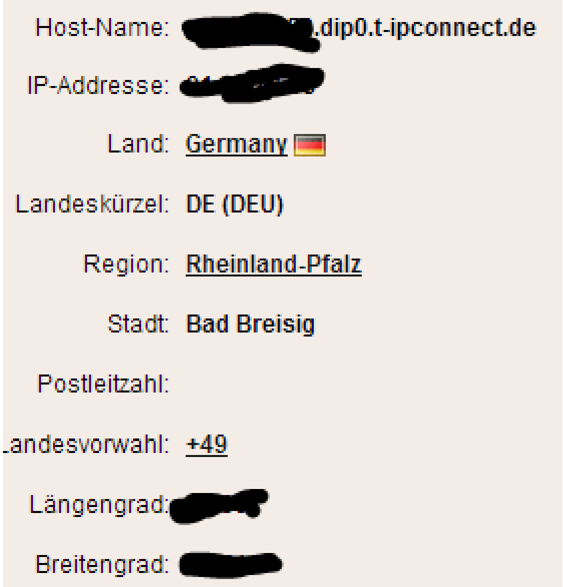
3. Confirming it is his IP

You are close to getting his IP, you might already have it but you do not know yet.

All you need to know now is in what country he lives or even better, in what state.

You can get that information by simple Social Engineering. Just ask him.

Go to http://www.geoiptool.com/ and enter his IP in the textbox.



Host-Name:	[redacted].dip0.t-ipconnect.de
IP-Addresse:	[redacted]
Land:	Germany
Landeskürzel:	DE (DEU)
Region:	Rheinland-Pfalz
Stadt:	Bad Breisig
Postleitzahl:	
Landesvorwahl:	+49
Längengrad:	[redacted]
Breitengrad:	[redacted]

Eventually it will dispense similar. I used my IP so I had to censor it for my own security.

If it says that he lives in that country you most likely got his IP.

But remember, anyone can use Proxys and VPNs and everybody can set his Skype profile country to anything.

And that's how you get an IP with Wireshark!

This method works on many peer to peer messengers!

Thanks for reading!

Made by Xaotic

http://www.hackforums.net/member.php?action=profile&uid=2105416