IP Adresse über ICQ sniffen:

Einige von euch (inkl. mir) nutzen ICQ zum Austausch von Informationen und privaten Gesprächen. Leider oder glücklicherweise (man nehme es wie es wolle!) kann man mit Hilfe alter DOS Befehle die IP via ICQ auf einem ganz einfachen Weg herausbekommen.

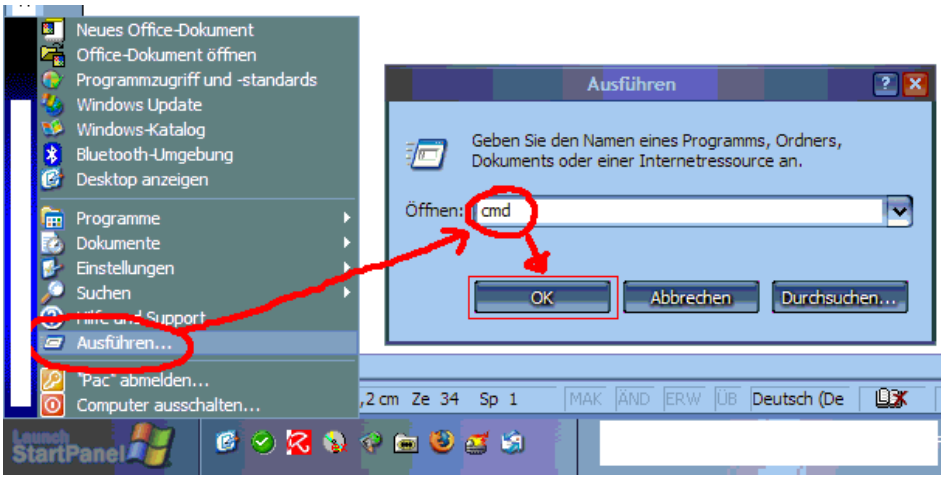
Vielleicht denkt jetzt der ein oder andere, dass seine IP sicher sei, da er
"Do not allow others to see my IP adress"
aktiviert hat. Leider ist dem nicht so, wie dieses Tutorial es euch hier Schritt für Schritt beweisen wird ;-)

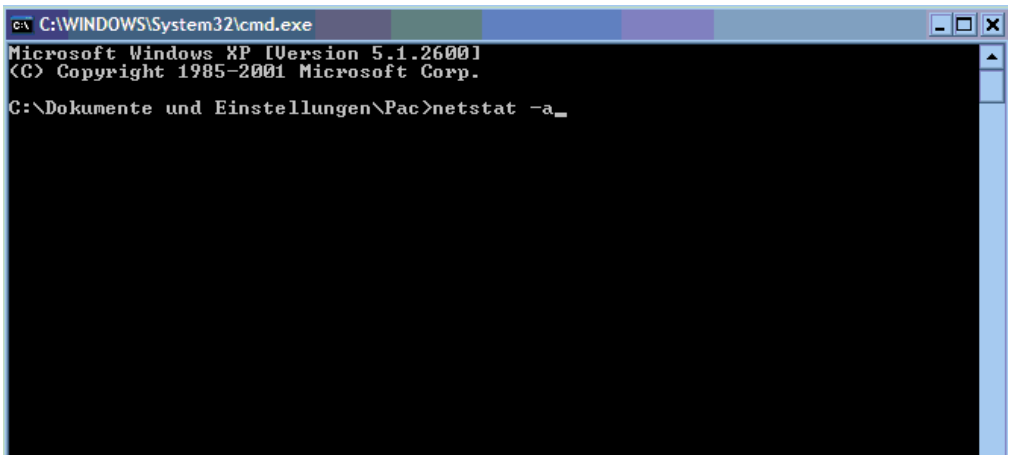
Schritt 1:

Schickt demjenigen eine Nachricht oder macht einen Chat auf, dessen IP ihr sniffen wollt
Öffnet sofort nach dem Versand der Message unter Windows die Dos-Eingabeaufforderung (Start -> Ausführen -> CMD) und tippt ein:

netstat -a

Netstat ist ein Programm, dass euch Protokoll Statistiken und aktive Netzwerkverbindungen anzeigt.





Schritt 2:
Nach einer Weile erhaltet ihr Informationen, die folgendermaßen aussehen können:

```
Active Connections
Proto Local Address Foreign Address State
TCP Demon:0 0.0.0.0:0 LISTENING
TCP Demon:1029 0.0.0.0:0 LISTENING
TCP Demon:1030 0.0.0.0:0 LISTENING
TCP Demon:1090 0.0.0.0:0 LISTENING
TCP Demon:1091 0.0.0.0:0 LISTENING
TCP Demon:1098 0.0.0.0:0 LISTENING
TCP Demon:1099 0.0.0.0:0 LISTENING
TCP Demon:1093 0.0.0.0:0 LISTENING
TCP Demon:1090 server5.sys.www.ozemail.net:80 CLOSE_WAIT
TCP Demon:1091 server5.sys.www.ozemail.net:80 CLOSE_WAIT
TCP Demon:1098 server5.sys.www.ozemail.net:80 CLOSE_WAIT
TCP Demon:1099 p3-max35.auck.ihug.co.nz:1054 ESTABLISHED
TCP Demon:137 0.0.0.0:0 LISTENING
TCP Demon:138 0.0.0.0:0 LISTENING
TCP Demon:nbsession 0.0.0.0:0 LISTENING
TCP Demon:1029 0.0.0.0:0 LISTENING
TCP Demon:1093 0.0.0.0:0 LISTENING
TCP Demon:nbname 0.0.0.0:0 LISTENING
TCP Demon:nbdatagram 0.0.0.0:0 LISTENING
```

Wie man aus diesen Informationen herausnehmen kann, besteht eine direkte Verbindung zu p3-max35.auck.ihug.co.nz:1054
Dies ist die aktuelle "Line" (also Leitung) die der User benutzt. Genau das ist es was uns interessiert.

Schritt 3:
Tippt in der Eingabeaufforderung ein: ping p3-max35.auck.ihug.co.nz:1054
Mit dem Befehl >ping. pingt ihr den User sozusagen an und guckt ob dieser aktiv ist
Das Ergebnis ist verblüffend und kann folgendermaßen aussehen:

```
Pinging p3-max35.auck.ihug.co.nz [209.76.151.67] with 32 bytes of data:
Reply from 209.76.151.67: bytes=32 time=1281ms TTL=39
Request timed out.
Reply from 209.76.151.67: bytes=32 time=1185ms TTL=39
Request timed out.
Ping statistics for 209.76.151.67:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 1185ms, Maximum = 1281ms, Average = 616ms
```

Na, ihr ahnt schon etwas ???? Die aktuelle IP Adresse unseres Opfers lautet: 209.76.151.67
Mehr steckt hinter einem solchen Sniffing nicht und ist doch supereinfach, oder ???

Zusatz:
Aber habt ihr Bock jedes Mal "netstat -a" und dann noch den langen host-name anpingen ??? Nein, denn wer hat schon Lust dazu. Dann versuch mal anstatt "netstat -a" einfach "netstat -n", da bekommst Du eine Liste mit IP's, mitdenen Du im Moment eine aktive Verbindung hast.
Und was man mit einer IP Adesse alles anfangen kann, muß ja von mir nicht weiter erläutert werden ;-)