



At finde en anden persons IP-adresse

Enhver Internetbruger har en IP-adresse, der i princippet kan spores tilbage til hans fysiske adresse. Artiklen ser nærmere på nogle metoder til at finde andres IP-adresse (fx en tyv, der har stjålet din PC), samt hvordan man kan surfe anonymt på nettet.

Skrevet den **03. Feb 2009** af **old-faithful** | kategorien **Netværk / Generelt** | ★★★★★

INDHOLDSFORTEGNELSE

1. Introduktion
2. Hvordan finder man sin egen IP-adresse?
3. Hvordan finder man en anden persons IP-adresse?
4. Hvad kan hjemmebrugeren finde ud af, ud fra en IP-adresse?
5. Anonymitet - Kan man holde sin IP skjult?
6. Diverse links
7. Svar på kommentarer + Ændringer

1. Introduktion

Når du bevæger dig rundt på Internettet (eller et netværk), har du en *IP adresse*, altså en »internet protocol« adresse. En IP-adresse svarer på mange måder til en almindelig postadresse. Således er en (ekstern) IP-adresse et unikt identifikationsnummer, som i princippet kan spores hele vejen tilbage til din hjemmearbejdsplads. Bl.a. har Politiet mulighed for at foretage sådanne sporinger, og det er på den måde, myndighederne kan finde frem til mange brugere af chathjemmesider m.m..

Privatpersoner ville også kunne spore en IP-adresse, men ikke helt tilbage ejers adresse. Derimod kan privatpersoner normalt se hvilket land IP-adressen hører hjemme i, og hvilket generelle geografiske område der er tale om.

En IP-adresse bruger formen: xxx.xxx.xxx.xxx (hvor xxx er et tal mellem 0-255). En IP-adresse kunne f.eks. være "98.132.97.43" (NB: opdigtet adresse).

Bemærk at en IP kan - afhængig af Internetudbyderen - være enten *statisk* (dvs. fast) eller *dynamisk* (dvs. kan ændres hver gang du logger på eller med faste intervaller; typisk tildeles en dynamisk IP af en DHCP-server men det er en helt anden sag).

Men hvornår er det så relevant at kende en anden persons IP-adresse?

Kerneområdet er tyverier. Hvis din computer bliver stjålet har du normalt ingen jordisk chance for at finde den igen. Men er du heldig, vil tyven tænde for computeren på et tidspunkt og gå på Internettet, og så kan du nogle gange få fat i IP-adressen, som Politiet så i princippet kan bruge til at spore computeren.

Eller det kan være du bare vil kunne tjekke, om folk taler sandt når de siger, at de er i det ene eller det andet land. Eller også vil du spille et online spil eller chatte direkte, med en person der ikke ved hvordan

han finder sin IP-adresse.

I det følgende benyttes ordet »modpart« om den person, hvis IP-adresse du ønsker at få fat i.

2. Hvordan finder man sin egen IP-adresse?

Du kan finde din egen eksterne IP-adresse ved at benytte en af de mange hjemmesider, der giver denne mulighed, f.eks. www.myip.dk eller www.whatismyip.com. Du kan også selv lave en sådan "IP-visningsside" ved at bruge JavaScript, PHP el. lign. (dette vil dog ikke blive gennemgået nærmere her).

Du kan finde din *interne* IP, ved at trykke på "Start" -> "Kør..." -> Skrive "cmd" -> Trykke på "OK" -> Skrive *ipconfig* -> og så taste ENTER. Denne artikel handler dog i det væsentlige om at finde eksterne IP'er.

3. Hvordan finder man en anden persons IP-adresse?

3.1. Få vedkommende til selv at finde sin adresse

Den letteste måde er naturligvis, at bede vedkommende om selv at finde sin IP.-adresse og så sende den til dig. Der findes som nævnt mange hjemmesider, der kan fortælle dig hvad din IP-adresse er, f.eks.

www.myip.dk

Dog vil dette næppe være en mulighed, hvis du f.eks. skal have IP-adressen på f.eks. den tyv der lige har stjålet din bærbare. Læs videre.

3.2. Installér et sporingsprogram

Er du smart, har du før computeren blev stjålet installeret et sporingsprogram. Dette er et program der kører på din computer - evt. skjult - og som sørger for at underrette dig, hvis computeren f.eks. ligepludselig bruger en anden IP-adresse end den sædvanlige.

Der findes flere sporingsprogrammer, der kan hjælpe dig. En del af dem koster penge, men der findes også gratis sporingsprogrammer, f.eks.:

- LocatePC (<http://www.locatepc.com/>)

- LostPC (<http://www.lostpc.com/>)

Du kan evt. også se på eMailMyIP, som jeg dog ikke selv har afprøvet (<http://www.scrammit.com/software.htm>)

Husk: Hvis det pågældende program sender en mail med oplysninger om IP'adressen, bør den stjalne computer ikke have umiddelbar adgang til denne mailkonto, da tyven ellers ville modtage mailen selv!

3.3. IP-adressen på MSN Messenger og andre direkte forbindelser

De metoder der nævnes herover, er nok de mest pålidelige. De følgende afsnit vil forklare mere specialiserede måder at opnå en persons IP-adresse på. Dette afsnit omhandler direkte forbindelse ("peer 2 peer"), som f.eks. MSN Messenger-filoverførsler.

3.3.1. At finde modpartens IP ved direkte forbindelser

1) I Windows vælger du "Start" -> "Kør..." -> Skriver *cmd* (eller *command*) -> Trykker på "OK"

2) Der kommer nu et DOS-vindue frem. Heri kan du skrive *NETSTAT -ANO* og trykke på ENTER for at få en oversigt over alle de forbindelser, din computer har oprettet. Vil du lægge denne oversigt i en fil kan du efter netstat-syntaksen skrive *>minlogfil.txt* eller lignende ("*>*" symbolet sørger for at lægge listen ned i en tekstfil og overskriver en eksisterende tekstfil af samme navn. Bruger du to af disse tegn "*>>*" vil listen derimod tilføjes til en eventuelt eksisterende tekstfil)

NB:

- Netstat findes kun på Windows NT-baserede systemer, som Windows XP, Windows 2000 og 2003. Netstats funktioner afhænger af hvilket styresystem man benytter. Windows 2000 understøtter således ikke "-o" funktionen (i stedet kan du bare bruge *NETSTAT -AN*).

- Du kan evt. bruge NetStatMon til at se hvornår forbindelser ændres/oprettes

(<http://www.hollmen.dk/content/view/74/31/>).

- Et alternativ til Netstat er Sysinternals' TcpView

(<http://www.microsoft.com/technet/sysinternals/Networking/TcpView.mspx>).

3) Læg mærke til hvilke forbindelser der er, når du ikke har oprettet en direkte forbindelse.

4) Opret så en direkte forbindelse til den, hvis IP du prøver at finde (I MSN oprettes der ikke direkte forbindelser, medmindre du sender en fil af en vis størrelse, f.eks. 1 MB).

5) Imens der er direkte forbindelse, bruger du nu igen *NETSTAT -ANO* for at se hvad modpartens IP-adresse er. Du kan nu sammenligne de to oversigter og finde modpartens IP-adresse

NB: Det vil selv sagt være svært at lokke en tyv til at modtage noget via MSN eller andre direkte forbindelser. Selv om det er usandsynligt, skader det dog næppe at prøve, f.eks. at lokke med noget som tyven vil have svært ved ikke at acceptere, pga. nysgerrighed eller grådighed (f.eks. en fil via MSN sammen med teksten "de frække billeder vi tog sammen sidst" eller lignende). Se dog først underafsnittet om MSN Messenger-overførsler før du bruger ovennævnte metode.

3.3.2. Typiske porte:

Programmer der bruger Internettet, benytter ofte visse porte. I netstat-oversigten, kan du se hvilken port der er tale om, ved at kigge på det tal der efterfølger en IP-adresse (med et kolon). Det flg. er en vejledende oversigt:

- 1863: MSN Messenger (men MSN kan benytte andre porte, f.eks. port 80, hvis den pågældende er blokeret)

- 6891 MSN Messenger filoverførsler (TCP)

- 13324-5: MSN Video og lyd

- 1503: MSN Messenger programdeling

- 4443: AIM, Yahoo filoverførsler

- 5190: AIM (standard, kan også være f.eks. port 20 - 23, eller 80)

- 5050: Yahoo (standard, kan også være f.eks. port 80)

Når du bruger *NETSTAT -AON* vil du også få vist en oversigt over *PID*'er ("Process ID"), som er et identifikationsnummer som kørende programmer har. Du kan finde ud af hvilket PID et program har, ved at sammenligne med det PID som vises i "Windows Jobliste" (få Windows Jobliste frem i Windows XP o. lign., ved at trykke på CTRL + ALT + DELETE en gang)

Du kan naturligvis eksperimentere med en anden *NETSTAT*-syntaks for at få andre detaljer vist, f.eks. *NETSTAT -anb* m.v. (Se syntaks-muligheder, ved at skrive *NETSTAT/?* i DOS-vinduet).

3.3.3. MSN Messenger-metoder

Det er set før, at tyve er logget på ofrenes MSN Messenger. Desuden kan det være, at du har brug for at kende en MSN-vens IP-adresse.

Normalt forbinder MSN Messenger ikke folk direkte, men via en server. I et sådant tilfælde er det formentlig ikke umiddelbart muligt at få modpartens IP-adresse. Men MSN Messenger er indrettet således, at der - når større filer sendes - oprettes en direkte forbindelse mellem afsender og modtager.

Dette faktum kan du udnytte ved at benytte den fremgangsmåde, som benyttes i afsnittet herover. Men der findes også en anden metode. Læs videre.

MSN Messenger - En anden metode:

NB: Denne forklaring bruger den engelsksprogede udgave af MSN Messenger, men finder naturligvis også anvendelse på den danske udgave; fremgangsmåden er tilsvarende.

En anden metode til at finde frem til modpartens IP-adresse i MSN Messenger er at:

- 1) trykke på "Tools" -> "Options" -> "Connection" -> "Advanced Settings...".
- 2) Sæt dernest flueben i "Save a log of my server connections to help troubleshoot connection problems".
- 3) Tryk så på "OK" og "OK". Send dernæst modparten en hvilken som helst fil (vent indtil modparten enten afslår eller accepterer overførslen).
- 4) Følg pkt. 1 for at deaktivere logfilen igen
- 5) Åben mappen "My Documents\Received Files" -> MsnMsgr ("Dokumenter\Modtagne filer").
- 6) Søg nu efter "connecttoip" og kig manuelt i teksten, efter IP-adressen

3.4. IP-adresser via en hjemmeside

Har du adgang til en hjemmeside, der logger oplysninger om dens besøgende, kan du bruge dette til at finde IP-adressen på din modpart.

Mange hjemmesider logger automatisk oplysninger om de besøgende, inkl. oplysninger om IP-adresse, browser version m.m. Dette er én mulighed, hvis du har adgang til hjemmesidens logfiler og har en nærmere måde at indkredse de besøgende, for at finde modparten.

Hvis du har din egen hjemmeside med f.eks. PHP-understøttelse (andre "sprog" vil naturligvis kunne benyttes, men i denne artikel nævnes kun en PHP-udgave), kan du også lave en side, der opsnapper IP-adressen på enhver der besøger pågældende side.

F.eks. kan flg. PHP-kode (lånt fra <http://www.dreamincode.net/code/snippet212.htm>) benyttes:

```
<?php
$logfile= '/full_path_to/log.html';
$IP = $_SERVER['REMOTE_ADDR'];
$logdetails= date("F j, Y, g:i a") . ' : ' . '<a
href=http://dnsstuff.com/tools/city.ch?ip='.$_SERVER['REMOTE_ADDR'].'>'.$_SERVER['REMOTE_ADDR'].'</
a>';
$fp = fopen($logfile, "a");
fwrite($fp, $logdetails);
fwrite($fp, "<br>");
fclose($fp);
?>
```

Dette kan indsættes et sted i en HTML fil (der så omdøbes til en .php fil) eller blot uploades. Enhver der så besøger siden, vil blive logget.

NB: Er der tale om en tyv der har fået adgang til din email eller MSN kan du igen være kreativ her, ved at

sende en besked/mail hvori der står noget i retningen af "*her er dine bankoplysninger, hent dem venligst snarest da jeg ikke vil have dem liggende for lang tid på serveren*" eller brug det ovennævnte "*frække billeder*"-trick. Det kan selvfølgelig ikke garanteres at tyven/modparten vil gå ind på siden, men gør han/hun det, klapper fælden.

Hvis du ikke regner med at du ville kunne få nogen til at gå ind på ovennævnte PHP-side, kan du (før computeren stjæles!) indbygge koden i f.eks. en hjemmelavet startside, og så vil IP-en logges hver gang nogen benytter den startside (hvilket jo som standard sker, hver gang man åbner f.eks. Internet Explorer). Bemærk, at dette kun virker, hvis PHP-filen ligger på en webserver/hjemmeside. Logfilen kan desuden blive ret stor efterhånden, så det kan være en god idé i givet fald, at nulstille den en gang imellem.

Der findes flere gratis hjemmesideudbydere, som understøtter PHP. Prøv f.eks. www.awardspace.com, som tilbyder gratis hjemmesider, med PHP og uden reklamer. Du kan evt. kombinere en gratis side, med en gratis viderestillingstjeneste som TK (<http://www.dot.tk/en/index.html>).

3.5. Emails - Finde afsenderens IP-adresse

I nogle tilfælde vil det være muligt at finde modpartens IP-adresse, hvis denne har sendt en email til dig eller en person du kender. En email gemmer nemlig oplysninger om IP m.v. i emailens "header" (dvs. et teksstykke i starten af mailen med tekniske detaljer, der normalt ikke bliver vist).

De fleste bedre emailprogrammer, ville kunne vise dig email headers. Bruger du f.eks. Outlook (engelsk udgave), kan du højreklikke på en email, vælge "Options" og så få vil du bl.a. få vist emailens header. Kig evt. efter det sidste sted i headeren hvor der står *Received: from*.

Email-metoden vil ikke altid være lige pålidelig. F.eks. virker den næppe hvis modparten har benyttet en gratis, webbaseret email-tjeneste som Hotmail eller Yahoo.

Der findes eftersigende også programmer som kan registrere modpartens IP-adresse når han åbner en mail.

3.6. Port-overvågningsmetoden

Endnu en mulighed er at få modparten til at trykke på et link, der henviser til den computer du bruger. Samtidig bruges en *port watcher* til at opfange IP-adressen på modparten, når denne prøver at forbinde til din computer.

Nogle gratis port watchers:

- Port Listener XP (<http://www.snapfiles.com/get/portxp.html>)
- Port Watcher 0.2 (af Thomas Harning, 2000):
<ftp://ftp.simtel.net/pub/simtelnet/win95/winsock/wtcher02.zip>
- Port Block (af Kurt Olstrom) <ftp://ftp.simtel.net/pub/simtelnet/win95/winsock/portblk2.zip>
- Roadkil's Detector (<http://www.roadkil.net/Detector.html>)
- Active Ports (<http://www.protect-me.com/freeware.html>)

NB: Der findes også "IP stealers", dvs. programmer lavet specifikt til nævnt formål, som benytter denne fremgangsmåde.

3.7. At få fat i en hjemmesides IP-adresse

Du kan også finde ud af, hvilken IP en hjemmeside har.

I Windows vælger du "Start" -> "Kør..." -> Skriver *cmd* (eller *command*) -> Trykker på "OK".

Herefter skriver du f.eks. `ping www.minside.dk/`

Så burde du kunne se, hvilken IP-adresse hjemmesiden har.

3.7. IP-adresser i fildelingsprogrammer m.m.

Ofte er der i fildelingsprogrammer o.lign. indbygget en mulighed for at se modpartens IP. Som regel skal man højreklikke på modpartens brugernavn el.lign. og vil så kunne få vist IP-adressen ved at vælge det relevante menupunkt. Se dit programs dokumentation for at se om det konkret er muligt i dit tilfælde.

4. Hvad kan hjemmebrugeren finde ud af, ud fra en IP-adresse?

Når du har fået fat i en ekstern IP-adresse kan du gå på lidt detektivarbejde-light. Man kan som nævnt (som regel) ikke selv finde modpartens fysiske hjemmeadresse (hvilket myndighederne normalt ville kunne), men man kan finde visse andre detaljer.

Du kan f.eks. finde hostname, ved at indtaste IP-adressen på flg. side:

- <http://www.myip.dk>

Ud fra et "hostname", kan du så finde ud af hvilket geografisk område, der er tale om. Hvad angår danske IP'er, kan du bruge den flg. "reverse dns" liste (til TDC adresser):

- <http://www.makr.dk/reversedns>

Listen er ikke komplet, så nogle gange kommer man ikke videre. Du kan dog prøve at se om der er et domænenavn (dvs. hjemmesideadresse) gemt i det fundne hostname.

Lad os tage et par eksempler:

Eksempel 1: Det fundne hostname er "stud-sp.cbs.dk". Kigger du nærmere herpå, kan du se at der optræder et domænenavn: "stud-sp.**cbs.dk**". Således indtaster du domænenavnet *cbs.dk* i Internet Explorer og så dukker hjemmesiden "Copenhagen Business School" op.

Eksempel 2: Du har via www.myip.dk eller lignende fundet et hostname der hedder "fw.oek.dk". Heraf kan du udlede et domænenavn "oek.dk", som du så skriver ind i Internet Explorers adressebar, og vupti, så kan du se at der er tale om Øresundskollegiet.

Et andet interessant værktøj, er et såkaldt "traceroute" program, der gør det muligt at se bl.a. hvilke servere en IP-adresse går igennem. Prøv f.eks. en online traceroute via <http://www.network-tools.com/> eller et af de flg. gratis programmer:

- TjPing: <http://www.topjimmy.net/tjs/>

- 3d Traceroute: <http://www.d3tr.de/index.html>

- Trout:

<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/prod/sc/trout.htm>

- PingPlotter Freeware: <http://www.pingplotter.com/standard.html>

5. Anonymitet - Kan man holde sin IP skjult?

Der findes visse metoder, der gør det sværere for andre at se din IP-adresse. Det betyder dels at du selv kan bruge en sådan mulighed for at gøre dine Internet-vaner mere anonyme, men også at andre kan bruge muligheden for at undgå at du får fat i deres IP-adresse.

Lad mig indledningsvist fastslå at total anonymitet er noget nær umuligt, men man kan stadig surfe relativt anonymt ved at bruge såkaldte "anonymous proxy servers". Hvor dine detaljer (såsom IP adresse) almindeligvis sendes med når du besøger en side eller opretter forbindelse til andre, og dermed kan logges, fungerer en proxy server som et mellemlid, hvormed din IP-adresse m.v. kan holdes hemmelig.

Normalt vil din Internet-færdse ske igennem en række servere der blot videresender det data der sendes frem og tilbage, f.eks.:

Din computer -----> ServerA -----> ServerB -----> Destination (f.eks. hjemmeside)

Men ved at bruge en anonym proxy server, indsætter man et led, som fjerner oplysninger om dig, f.eks. IP-adressen.

Din computer -----> ServerA -----> (Anonym proxy server) -----> ServerB -----> Destination

Proxy-serveren svarer lidt til en mand i mellem din computer og "destinationen". Denne mand sørger for at dit data sendes videre uden afsenderinformation og sørger for at sende data fra destinationen tilbage til dig igen.

Således bliver man anonym på nettet, og f.eks. den hjemmeside du besøger, kan ikke se din IP-adresse.

Systemet er dog ikke uden svagheder. Det forudsættes naturligvis at du benytter en proxy som du kan stole på (selv kan de på proxy-serveren se dine data, medmindre de er krypterede) og som ikke gemmer trafiklogs. Ellers kan ejeren af serveren se hvem bruger serveren, samt hvad sendes frem og tilbage, og serverens log kan evt. kræves udleveret af myndighederne (afhængig af lovgivningen i landet hvor serveren ligger). Desuden er det set i praksis, at ondsindede mennesker har oprettet proxy servers og brugt dem til at opsnappe godtroende brugeres personlige kodeord og oplysninger i øvrigt.

Problemet med proxy servere er således, fra brugerens synspunkt, at vedkommende skal være fuldstændig sikker på at han kan stole på pågældende proxy server. Den kan jo være sat op af tyve og bedragere, eller af fremmede landes myndigheder el. lignende.

Der findes hjemmesider som kan fungere som proxy servere, men også programmer der kan koble dig op til proxy servere. Mange Internetprogrammer (f.eks. Internet Explorer) kan sættes op til at køre igennem en proxy, enten direkte eller igennem et program på din computer (som regel skal proxy'en så angives som "localhost" eller 127.0.0.1), der finder og kobler dig til proxy servers.

I Internet Explorer kan man f.eks. sætte programmet til at forbinde igennem en proxy, ved at vælge "Funktioner" -> "Internetindstillinger" -> "Forbindelser".

Bemærk at der også er forskel på hastigheden af de forskellige proxy servere, så forbindelsen kan være endda meget langsom nogle gange. Desuden vil en proxy server ikke pr. definition anonymisere noget medmindre det er en "anonym" proxy server (en transparent proxy server skjuler ikke noget).

Herefter følger nogle proxy-relaterede links, som dog ikke vil blive uddybet nærmere i denne fremstilling.

Nogle proxy-relaterede softwareprogrammer:

- ☐ Torrify (<http://www.torrify.com/>)
- ☐ OperaTor (<http://letwist.net/operator>)
- ☐ Multiproxy (<http://www.multiproxy.org/>)
- ☐ Anonymous Guest Pro 4 (<http://www.spszone.com/anguet/>)

- Tor (<http://tor.freehaven.net/>)
- Proxy-Firewall (<http://proxy-firewall.com/>)
- Proxyrama (<http://gaamoa.deny.de/index.html>)

Hjemmeside-baserede proxy servers:

- Proxify (<http://proxify.com/>)
- Megaproxy (<http://www.megaproxy.com/freesurf/>)
- The Cloak (<http://www.the-cloak.com/login.html>)
- Anonymouse

6. Diverse links

Find din egen IP m.v.:

- <http://www.myip.dk>
- <http://www.whatismyip.com/>

Online traceroute m.v.:

- <http://www.network-tools.com/>

7. Svar på kommentarer + Ændringer

Jeg modtager gerne forslag, kommentarer og *begrundede* karakterer, så jeg løbende kan forbedre artiklen.

Ændringer:

- 23. december 2006: Stave- og grammatikfejl rettet, samt tilføjet henvisning til NetStatMon
- 22. december 2006: Tilføjet bemærkning om NETSTAT ang. forskellige udgaver af Windows
- 21. december 2006: 1. udgave

Svar på kommentarer:

kenp:

Tak. Jeg har tilføjet en bemærkning om NETSTAT og Windows-versionerne.

imago-dei:

Vil du ikke uddybte hvad du mener med at man ikke bare kan sætte "sin pc til at bruge en tilfældig IP-adresse" og ikke kan "komme på nettet hjemme hos mig med din faste ip adresse"? Det har vist ikke skrevet noget om?

thomaxz :

Er der noget du synes kunne forbedres ved artiklen?

Kommentar af coderdk d. 12. Jan 2007 | 1

Et andet alternativ for anonymitet er relakks: <https://www.relakks.com/?cid=gb>

Kommentar af bug30 d. 23. Dec 2006 | 2

Rigtig go læsning.

Kommentar af boheme d. 26. Dec 2006 | 3

Kommentar af greew d. 01. Jan 2007 | 4

Ganske fint. Langt det meste vidste jeg i forvejen, men det er jo altid bruge at få det genopfrisket :)

Kommentar af kenp d. 22. Dec 2006 | 5

God artikel.

Kommentar af sarkis d. 04. Jan 2007 | 6

Meget vel forklaret!

Kommentar af htmlkongen d. 22. Dec 2006 | 7

Detaljeret og meget godt beskrevet. Er "ny" på området så kan ikke give yderligere kritik. Bestemt værd at læse. Noget at lære for enhver /Htmlkongen

Kommentar af imago-dei d. 10. Jan 2007 | 8

God artikel. Mange gode små tips. Men jeg betvivler lidt metoden til at finde sin computer tilbage via fast ip hvis den bliver stjålet. For det første er der de færreste som har en fast ip (gætter jeg på), og for det andet kan man ikke bare sætte sin pc til at bruge en tilfældig ip adresse. Mao. jeg kan ikke komme på nettet hjemme hos mig med din faste ip adresse.

Kommentar af mrgumble d. 06. Jan 2007 | 9

God og uddybende artiekl. Thumbs up!

Kommentar af bdai d. 14. Jun 2008 | 10

Kommentar af swiatecki d. 21. Dec 2006 | 11

C'est tres bien :D

Kommentar af thomaxz d. 10. Jan 2007 | 12

Kommentar af psycosoft-funware d. 25. Dec 2006 | 13

jeg har ikke andet at sige at det er super godt skrevet :D
thumbs up, keep up the good work :)

Kommentar af egebos d. 27. Jan 2007 | 14

Kommentar af califfo d. 27. Dec 2006 | 15

Smuk. Lærerig.

Kommentar af windcape d. 22. Dec 2006 | 16

Godt skrevet :) Jeg vil anbefale Tor til ip-disguise.

Kommentar af bassehunden d. 25. Jan 2007 | 17

God og lærerig artikel, spændende læsning

Kommentar af jenniferj d. 20. Nov 2007 | 18

Kommentar af stebit d. 05. Sep 2012 | 19

Rigtig godt forklaret, tak.

Kommentar af ClausMikkelsen d. 03. Jul 2013 | 20

Mange tak, jeg fik god information.

Claus

www.hotpaper.dk

Kommentar af MichaelBFrost d. 03. Jul 2015 | 21

Tak for en god og udførlig vejledning :)

Med venlig hilsen

Michael Frost

www.lajlaboe.dk

Kommentar af Michael_Svensen d. 14. Aug 2015 | 22

Virkelig god og udførlig guide. Stor thumbs up herfra!

Kommentar af arne123 d. 18. Aug 2015 | 23

Tak for en god guide!

Kommentar af madskobenhavn d. 30. Dec 2015 | 24

Super god guide. Mange tak for det ! :)