Reiko Kaps, Noud van Kruysbergen

# Verkeerscontrole

## Foutopsporing, netwerkanalyse en Eerste Hulp met de c't-Netwerktoolkit

**Het is uitermate irritant als je pc niet meer op het netwerk kan of de internetverbinding er de hele tijd uitligt. De tools op onze cover-dvd en in de c't-Netwerktoolkit kunnen je helpen erachter te komen wat er precies mis is.**

Zonder netwerk en internet wordt het lastig om de juiste tools te vinden om een verbindingsprobleem op te lossen. Daarom hebben we een aantal programma's gebundeld die direct vanaf een usb-stick gestart kunnen worden en dus niet eerst geïnstalleerd hoeven worden. De verzameling vormt daarmee een handige aanvulling op de standaardfunctionaliteit van het besturingssysteem. Met deze tools kunnen netwerkfouten in routers, pc's of draadloze netwerken makkelijk worden gevonden en verholpen.


Na het uitpakken in de rootmap van een geheugenstick nemen alle programma's in de toolkit nog geen 300 MB in beslag. Ze starten via een eenvoudig menusysteem of via een reeds ingerichte commandline. Eigen aanpassingen voor de commandline kun je opgeven via de menuoptie 'Commandline instellen' in de configuratie. Je kunt met de muis zelf nieuwe dingen toevoegen in het menusysteem.

### Contactarm

Als je pc van het ene op het andere moment niet meer op internet wil, is het verstandig om eerst te controleren of alle aansluitingen wel functioneren: zit de ethernetkabel in de switch of router en in de netwerkkaart van de pc en knipperen de controleleds? Als je zeker weet dat er geen kabels defect zijn of ontbreken, dan laten de standaardtools van Windows zien wat het besturingssysteem met een netwerk kan.

Onder Windows zijn naast de grafische tools in het Netwerkcentrum ook een aantal commandlinetools zoals ipconfig beschikbaar. Dit commando laat zien of de ethernetkabel er goed in zit en geeft een overzicht van de IP-configuratie voor echte en virtuele netwerkinterfaces:

```
ipconfig.exe
Ethernet-adapter tinc-vpn:
   Mediastatus : medium ontkoppeld
   Verbindingsspec. DNS-achtervoegsel : example.com
Ethernet-adapter LAN-verbinding:
   Verbindingsspec. DNS- achtervoegsel : test.fnl.nl
   Link-local IPv6-adres : fe80:7de9:e6ee:73b2:ceb6%10
   IPv4-adres : 192.168.178.104
   Subnetmasker : 255.255.255.0
   Standaardgateway : 192.168.178.1
```

Als de netwerkkaart 'tinc-vpn' het niet doet (Mediastatus: medium ontkoppeld), verbindt de pc zich via de ethernetadapter 'LAN-verbinding' met het adres 192.168.178.104 aan het lokale netwerk. Als deze pc pakketten naar computers wil sturen die niet bij het lokale netwerk horen, stuurt hij ze naar het adres 192.168.178.1. Deze standaardgateway stuurt deze requests verder door internet. Bovendien geeft ipconfig via het 'Link-local IPv6-adres' aan dat de computer in principe met IPv6 overweg kan.

In het overgrote deel van de gevallen haalt de computer deze informatie via DHCP automatisch van de router, die in kleine netwerken vaak ook als standaardgateway dient. Een request via de overal aanwezige tool ping laat zien of de verbinding tot daar ook werkt: de ping van Windows verstuurt na de invoer van ping 192.168.178.1 vier requests en analyseert de antwoorden.

Als ping daarbij geen fouten meldt, dan werkt de lan-verbinding. In de c't-Netwerktoolkit zit nog de pingvariant **fping**, waarmee je bij meerdere adressen kunt aankloppen. Dit programma werkt in de opdrachtprompt van Windows en start zonder installatie en heeft veel extra switches om onder andere de tijdvariantie (jitter) tussen de antwoorden te bepalen (-j) of een tekstbestand met doeladressen mee te geven (-H). Bij een aanroep zonder parameters zie je alle opties. De **eToolz** van Werner Rumpeltesz zijn makkelijker te bedienen, maar beperkt tot het hoogst noodzakelijke, zijn. Deze ondersteunen helaas geen IPv6.

Als ping of fping bij een aanroep met de hostnaam www.ct.nl fouten melden als 'No route to host' of 'unreachable address', moet de fout wellicht gezocht worden in het Domain Name System. Probeer het dan rechtstreeks met ping 213.206.247.69. Als dat foutloos werkt, wordt het tijd eens naar het DNS te kijken.

## Geen informatie

De servernaam www.ct.nl komt overeen met een numeriek IP-adres dat programma's via het Domain Name System (DNS) kunnen opvragen: als je de naam in de browser invoert, vraagt die de verantwoordelijke DNS-server naar het IP-adres. Als het DNS vervolgens een IP-adres teruglevert, maakt het programma de verbinding. Zo niet, dan meldt de software 'server niet gevonden', maar meestal zonder verdere details.

Het opsporen van de fout kan versneld worden met hulpmiddelen als het Windows-programma nslookup en het commando **host**.

```
nslookup www.ct.nl
Server: UnKnown
Address: 192.168.0.6

Niet-bindend antwoord:
Naam: magazines.fnl.nl
Address: 213.206.247.69
Aliases: www.ct.nl
```

Het commando laat zien welke DNS-server voor het lan verantwoordelijk is en geeft daarna diens antwoord op de hostnaam www.ct.nl. In dit voorbeeld werkt op de router een DNS-proxy, die de requests doorgeeft aan de DNS-server van de internetprovider. Als je ter controle een andere DNS-server wilt gebruiken, bijvoorbeeld de servers van Google die via de adressen 8.8.8.8 en 8.8.4.4 bereikbaar zijn, dan geef je een van deze adressen achter de gezochte hostnaam mee aan nslookup (`nslookup www.ct.nl 8.8.8.8`. Als je nslookup zonder parameter start, kun je interactief via de commandline gebruiken. Typ dan 'help' in om een overzicht van de mogelijkheden te krijgen. Het commando `host` uit de **BIND-Tools** werkt makkelijker. De portable versie zit in de netwerktoolkit op de cover-dvd. Het commando `host www.ct.nl 8.8.8.8` laat in tegenstelling tot nslookup ook zonder parameters alle IP-adressen uit die in het DNS zijn opgeslagen, ook die voor IPv6.

In de BIND-tools zit ook het commando `dig` dat de ruwe en op het eerste gezicht onoverzichtelijke DNS-antwoorden laat zien. Die geven meer prijs over over DNS-aliases en de verantwoordelijke mail- en DNS-server. Met `dig www.ct.nl @8.8.8.8`. doe je een request voor www.ct.nl via de DNS-server 8.8.8.8. De invoer van `dig ct.nl mx` levert de verantwoordelijke mailserver voor het domein ct.nl. De DNS-server zou hierop moeten antwoorden met onder andere de regel

```
ct.nl. 716 IN CNAME magazines.fnl.nl.
```

Met dit hulpmiddel kun je snel de antwoorden van je eigen DNS-server vergelijken met die van andere DNS-servers. Bij een aantal internetproviders beantwoorden de standaard ingestelde DNS-servers niet-bestaande servernamen niet zoals verwacht met een foutmelding, maar leiden ze dit soort requests in plaats daarvan door naar eigen servers. Dat brengt een aantal netwerkprogramma's volledig in de war: met foutmeldingen zouden ze nog wat kunnen, maar de schijnbaar bereikbare servers leveren geen bruikbare gegevens terug. Dit gedrag kan bij een aantal internetproviders worden uitgeschakeld, maar dan moet je wel eerst weten dat daar de fout zit.

Een omleiding valt snel op: een DNS-server moet voor bijvoorbeeld zzz.ct.nl geen IP-adres teruglevert, maar een foutmelding als "; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id:24661". Een DNS-server met 'navigatiehulp' van buiten antwoord met een adres.

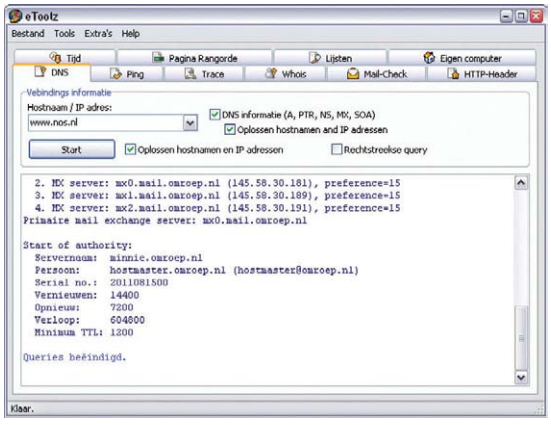
De door Google mede ontwikkelde software **namebench** test de snelheid van de eigen en andere publiek toegankelijke DNS-servers bijna volledig automatisch. Het programma vergelijkt de antwoorden van meerdere DNS-servers en noteert de daarvoor benodigde tijd. Dat levert veel details op die het bovendien grafisch getoond worden. De drie snelste DNS-servers zijn te zien, de details van de test staan in een tabel en de resultaten worden in een grafiek gezet.

## Laat me d'r uit!

Als je eigen computers met elkaar en met de router kunnen praten, maar aanroepen van externe webservers of diensten als Twitter ondanks een werkend DNS mislukken, kan het aan de routing liggen.

De pc stuurt alle netwerkpakketten die niet bestemd zijn voor het lokale netwerk naar zijn standaardgateway. Die geeft ze door aan de internetprovider, waar ze via verschillende tussenstations uiteindelijk op de juiste bestemming aankomen. Als deze route ergens gestremd is, gaan de requests verloren hoewel het correcte IP-adres van de doelcomputer bekend is.

Voor een uitgebreidere diagnose maak je ook dit keer weer eerst gebruik van een aantal tools van het besturingssysteem. Het commando `tracert` onder Windows achterhaalt via welke routers gegevens naar een doelcomputer worden gestuurd. Windows is vanaf Vista bovendien standaard voorzien van het commando `pathping`, dat meer details levert over hoe de pakketten naar de tussenstations worden gestuurd. Pathping verstuurt voor dit doel regelmatig pings naar alle gevonden tussenstations op de route en analyseert hun antwoorden.




**Met eToolz heb je traceroute, ping en nog veel andere netwerktools voor IPv4 in één interface. IPv6 ondersteunt hij niet.**

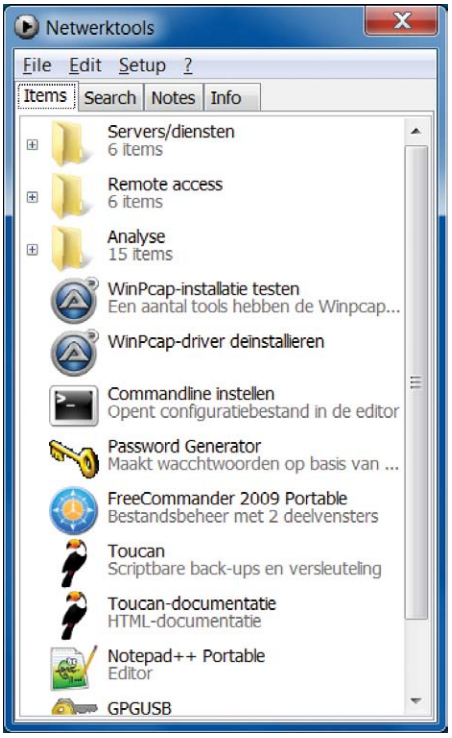
Het commando `mtr`, dat in veel Linux-distributies zit maar ook achteraf geïnstalleerd kan worden, werkt op een vergelijkbare wijze. **WinMTR** is een versie voor Windows die niet geïnstalleerd hoeft te worden.

Als bij het testen met deze programma's veel pakketten onderweg blijven steken, dan duidt dat op langzame verbindingen en verklaart dat de toegenomen foutmeldingen.

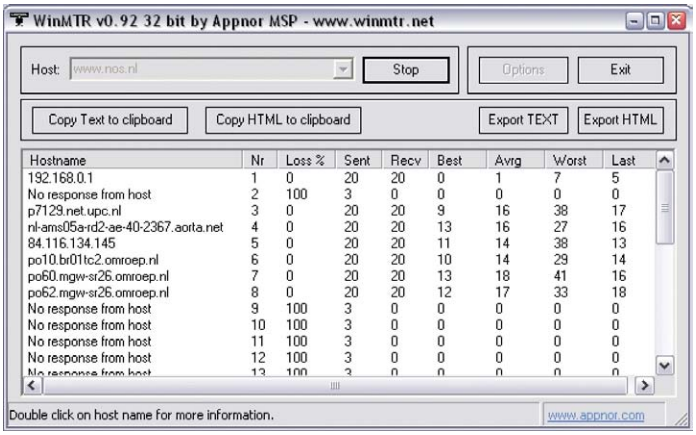
Als je wilt uitsluiten dat de problemen veroorzaakt worden door je eigen internetverbinding, dan helpt een online pingfunctie als http://ping.eu/ping. Die stuurt ping-requests nog alleen via IPv4 vanaf zijn webserver naar internet.

## Leven in het lan

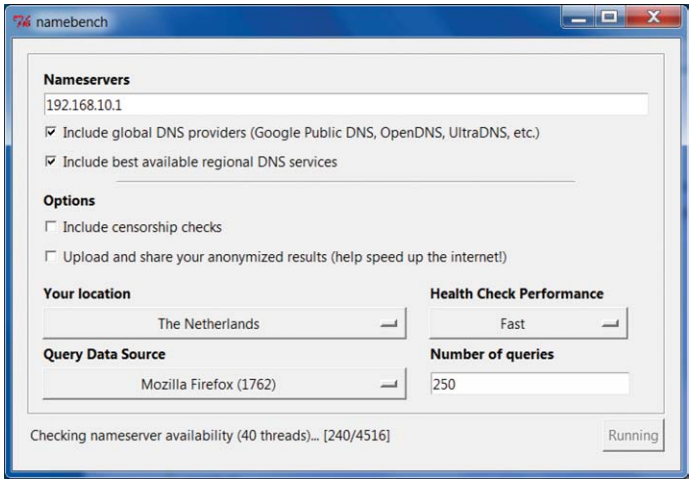
Als een computer niet op pings reageert omdat bijvoorbeeld zijn firewall ICMP-requests opslokt, kan hij nog altijd worden onderzocht. Netwerkscanners lopen de applicatiepoorten op een IP-adres af. Ze versturen daarbij korte requests en leggen de reactie daarop vast.




**De c't-Netwerktools hebben een eigen menu en een aangepaste opdrachtprompt voor tekstprogramma's.**




**WinMTR controleert op gezette tijden de kwaliteit van een verbinding naar een bepaald doel.**




**De DNS-benchmark namebench achterhaalt trage DNS-servers, DNS-vervalsers en laat snelle alternatieven zien.**

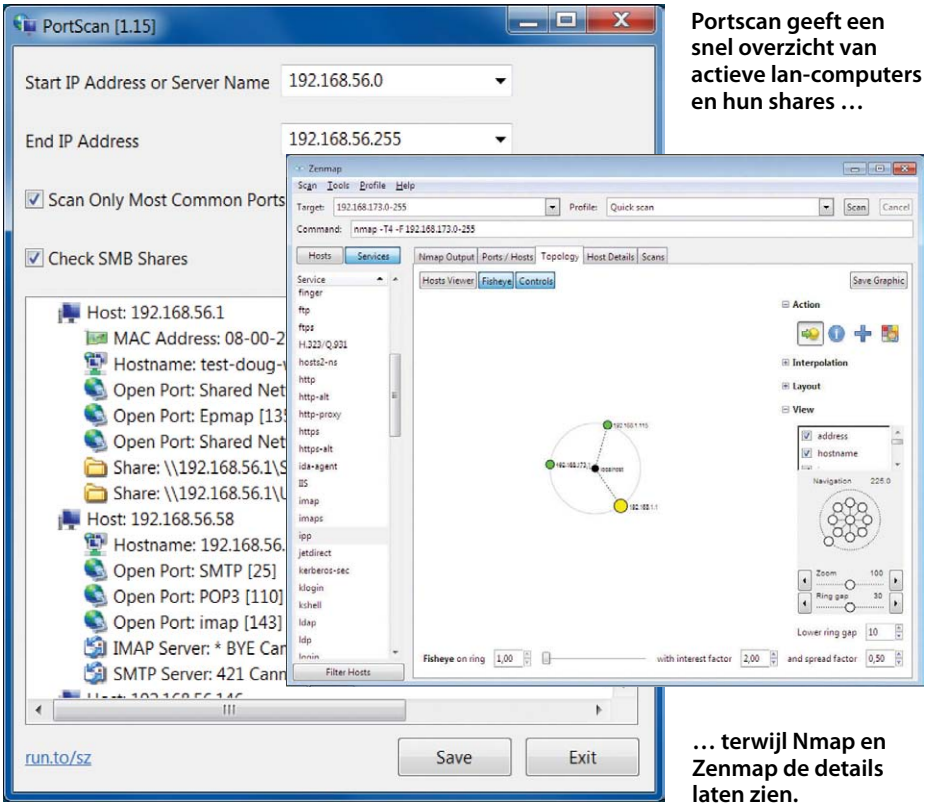
Eenvoudige varianten van deze softwarecategorie zoals het programma **PortScan**, dat niet geïnstalleerd hoeft te worden, testen hierbij de poorten voor het Windows-netwerk, ftp-, mail- en webservers, terminalservices en SNMP en laten ook meteen de bereikbare Windows-shares zien. De **Softperfect Network Scanner** biedt nog meer mogelijkheden en herkent niet alleen computers, MAC-adressen en netwerkdiensten, maar vindt ook DHCP-servers en UPnP-apparaten in het lan en achterhaalt het externe IP-adres van het lokale netwerk. Het programma laat IPv6-adressen zien, achterhaalt de Windows-versie, de netwerkgroep, de sharenamen en nog veel meer informatie.

Als de mogelijkheden van PortScan en Softperfect Network Scanner niet voldoende zijn, kun je je toevlucht nemen tot **Nmap**, het Zwitserse zakmes onder de netwerkscanners. De Windows-versie heeft de grafische interface Zenmap, waarmee je de invoer en doeladressen, maar ook het scantype makkelijk kunt instellen. Zenmap slaat deze instellingen voor later gebruik op als profiel. De Nmap-ontwikkelaars leveren een aantal voorbeeldprofielen mee.

Als je het lokale netwerk op actieve computers wilt doorzoeken, geef dan het adresbereik op (192.168.0.1-254), selecteer de snelle scanmethode (Quick scan) en start het zoeken via de knop 'Scan'. Tijdens het zoeken laat Nmap op het tabblad 'Nmap Output' zien wat hij gevonden heeft. Gevonden computers en diensten belanden in de lijsten links ernaast. Als je op het tabblad 'Services' bijvoorbeeld op de entry 'ipp' klikt, geeft Zenmap rechts alleen de IP-adressen die printservices via het Internet Printing Protocol aanbieden. Op het tabblad 'Topology' zit een extra tool verborgen die uit de scanresultaten een interactieve grafiek genereert.

Nmap en de programma's Wireshark, Windump en Ngrep, die we verderop in dit artikel nog zullen bespreken, hebben voor een aantal van hun functies bovendien de driver **WinPcap** nodig. Deze helpt de programma's bepaalde protocollen van de netwerkkaart af te luisteren die Windows anders niet zou prijsgeven.

De driver is niet geschikt om op een stick te zetten, hij moet per se geïnstalleerd worden. Twee menuopties in de c't-netwerktools helpen je echter bij het installeren of latere deïnstalleren van WinPcap.




**Portscan geeft een snel overzicht van actieve lan-computers en hun shares …**

**… terwijl Nmap en Zenmap de details laten zien.**

## Kabel afluisteren

Welke programma's 'bellen naar huis'? En wie wil er op dit moment vanuit internet of het lan op mijn computer? Dat kun je je bijvoorbeeld afvragen als je internetverbinding zonder duidelijke reden niet vooruit te branden is. Al gauw duikt het vermoeden op dat een schadelijk programma de controle over de computer heeft overgenomen. Windows of Linux zijn voor een eerste controle voorzien van het commando netstat.

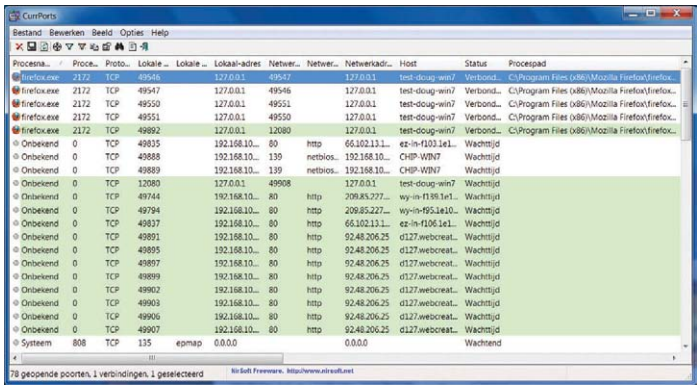
In de Windows-opdrachtprompt somt netstat met de parameters -ba naast de geopende poorten ook de programma's op die de betreffende verbinding opbouwen. Omdat deze lijst meestal erg lang is, verlies je al snel het overzicht. Het grafische **CurrPorts** maakt dat overzichtelijker met filters voor afzonderlijke programma's, poorten, IP-adressen en andere kenmerken. De uitvoer wordt bovendien als HTML opgeslagen en nieuwe verbindingen komen in een

logbestand. Bovendien kunnen via het snelmenu verdachte verbindingen en processen worden verbroken.

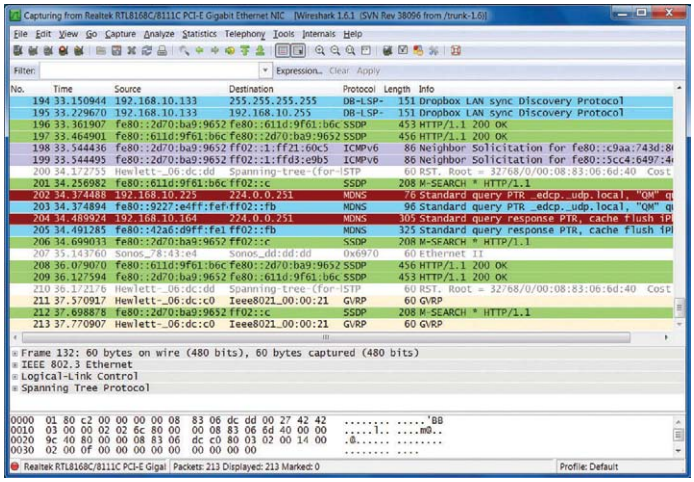
Wat er precies in deze verbindingen gebeurt en welke gegevens via deze verbindingen worden verstuurd, is alleen te achterhalen met een snifferprogramma. **Socketsniff** hangt zich bijvoorbeeld aan een werkend programma en laat in ongecodeerde tekst zien welke verbindingen er worden opgebouwd en wat de requests en reply's waren – als die tenminste niet versleuteld zijn. Dit soort informatie is nuttig als netwerktoepassingen niet met een server communiceren zoals je verwacht. De mailclient weigert bijvoorbeeld hardnekkig om met de mailserver te communiceren of je nieuwste eigen ontwikkeling zet in plaats van de laatste Flickr-foto's alleen een datachaos op het scherm.

Socketsniff werkt los en hoeft niet geïnstalleerd te worden. Bij het starten vraagt hij welke van de draaiende Windows-processen hij moet afluisteren. Sessies worden als HTML opgeslagen en de achterhaalde gegevens kunnen doorzocht worden. Het programma houdt onder 64-bit Windows echter alleen 32-bit software in de gaten.

Socketsniff-producent Nirsoft biedt ook het gratis Smartsniff aan dat zonder extra (Winpcap-)driver netwerkverkeer via rawsockets registreert. **Smartsniff** damt de af te luisteren netwerkgegevens bij het opnemen al in met filters, exporteert de informatie van afzonderlijke of bij elkaar horende pakketten (streams) als HTML- of tekstbestand en slaat de gelogde data in een eigen formaat op. Als Smartsniff zonder Winpcap-driver werkt, zijn echter niet altijd alle functies beschikbaar.



**Curports geeft net als het commandlineprogramma netstat in zijn interface een overzicht van openstaande verbindingen.**

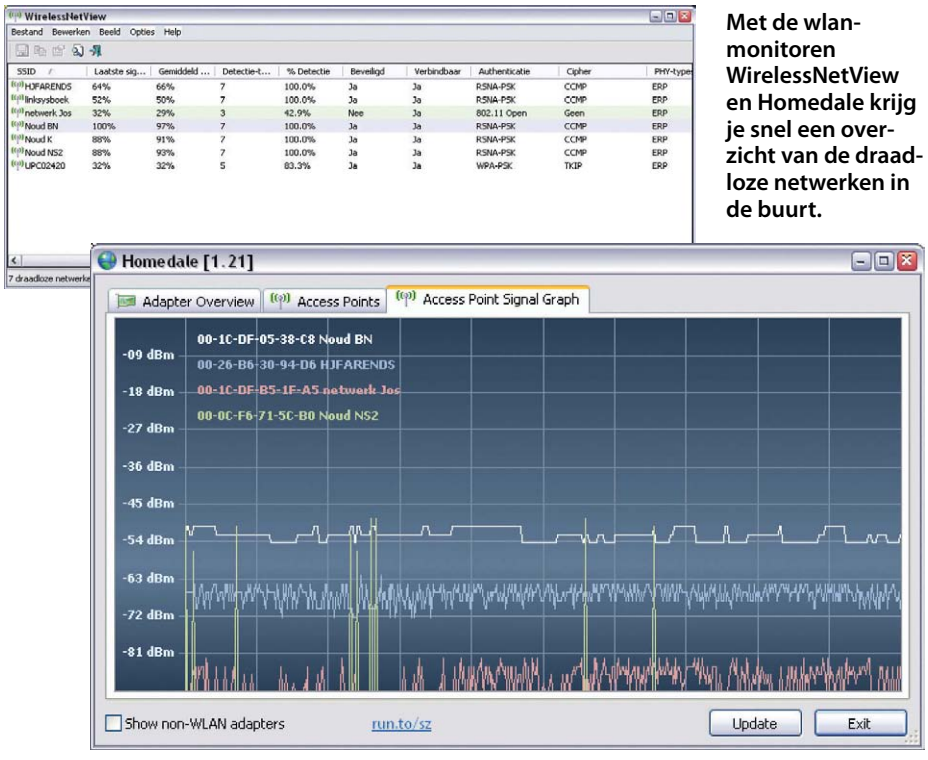


**De netwerksniffer en -monitor Wireshark doorzoekt het netwerkverkeer met filters op interessante pakketten. Voor het afluisteren heeft hij de WinPcap-driver nodig.**

**Wireshark**, de Mercedes onder de netwerksniffers, heeft voor het afluisteren per se de WinPcap-driver nodig. Als die geïnstalleerd is, start je een afluistersessie ofwel via de optie Interfaces in het Capture-menu of via de toetscombinatie Ctrl+I. Het loggen kan bovendien op het hoofdscherm in gang worden gezet – in dat geval zonder verdere navraag.

Als je er alleen bepaalde netwerkpakketten uit wilt vissen, stel je voor het starten bij de 'Capture / Options' een filter in dat het opnemen bijvoorbeeld beperkt tot pakketten naar HTTP-poort 80 'HTTP TCP port (80)'. Als Wireshark het netwerkverkeer van andere computers in het lan in de gaten moet houden, moet je een vinkje zetten bij 'Capture packets in promiscuous mode' – anders verwerpt de netwerkkaart van de computer pakketten die niet direct aan hem gericht zijn. Wireshark verzamelt na de start alle binnenkomende pakketten en laat die in het hoofdvenster zien. De weergave kan aan de hand van een groot aantal criteria in het Filter-veld tot alleen het interessante netwerkverkeer worden beperkt. Met `http.content_type matches "image/*"` krijg je alleen de HTTP-pakketten zien die verantwoordelijk zijn voor de overdracht van afbeeldingen.

Als je alle pakketten tussen twee computers wilt bekijken, klik je een filter met bron- en doeladressen bij elkaar: selecteer met de muis een pakket, klik met de rechtermuisknop op het doeladres en selecteer in het muismenu 'Prepare a Filter' en een van de snelkoppelingen. De knop 'Apply' activeert vervolgens het weergavefilter. Voor uitgebreidere filters kun je het beste het invoermasker achter 'Expression…' gebruiken. Voorgedefinieerde expressies helpen bij het maken van een filter en via de functie 'Follow TCP Stream' volgt Wireshark de datastroom




**Met de wlan-monitoren WirelessNetView en Homedale krijg je snel een overzicht van de draadloze netwerken in de buurt.**

van bij elkaar horende pakketten. De zeer gebruiksvriendelijke Wireshark-interface draait ook zonder WinPcap-driver, maar is dan alleen geschikt voor het analyseren van reeds opgeslagen data.

De twee consolesniffers **windump** en **ngrep** zoeken zonder extra parameter zelfstandig een netwerkinterface op de computer uit, die ze vervolgens afluisteren. Als je een specifieke interface opgeeft, dan laat Windump met de optie -D en Ngrep met -L een lijst zien van de aanwezige interfaces inclusief de bijbehorende interface-index. Dat nummer kun je meegeven aan windump achter de optie -i, bij Ngrep moet je dat achter de parameter -d zetten.

Windump laat zonder extra opties alleen de pakketheaders in de opdrachtprompt zien. Met `-w sessie.pcap` leid je de onderschepte pakketten om naar het bestand sessie.pcap. Met de parameter `-s 0` slaat Windump slaat dan de complete pakketten op. Bij Ngrep leidt `–O sessie.pcap` pakketten om naar het bestand sessie.pcap.

Eenmaal opgeslagen pakketten worden door Windump met -r en door Ngrep met -I weer ingelezen, zodat je ze met de filterfuncties van beide programma's kunt onderzoeken. Een eenvoudige aanroep van Ngrep en Windump om naar pakketten naar een HTTP-server (poort 80) te zoeken, luidt `ngrep -i interface-index dst port 80` respectievelijk `windump -d interface-index dst port 80`. Ngrep kan in de netwerkpakketten bovendien naar tekenreeksen zoeken: `ngrep … -wi "password|username" dst port 80`. Een aantal functies van Windump en Ngrep kunnen alleen gebruikt worden met een geïnstalleerde WinPcap-driver.

## Draadloze kunst

Windows geeft zeer beperkte informatie over draadloze netwerken in de buurt. Over wlan's zonder SSID zwijgt het besturingssysteem volledig. Daar springen wlan-scanners op in. Zij geven bovendien belangrijke informatie om je eigen draadloze netwerk optimaal aan de lokale omstandigheden aan te passen.

**Wirelessnetview** toont de kanalen, frequenties en de signaalsterkte van de omringende wlan's op de 2,4- en 5GHz-band op overzichtelijke wijze. De verzamelde informatie wordt opgeslagen als HTML-, XML-, CSV- of tekstbestand. Een aantal opties zoals het opslaan zijn via switches op de commandoregel bereikbaar.

**Als je een vrij gaatje tussen de wlan's zoekt, helpt de wlan-scanner inSSIDer2 met duidelijke grafieken bij het kiezen van een kanaal.**

Het portable **Homedale** zet de signaalsterkte van geselecteerde basisstations in een tijdsgrafiek. **Wirelessnetconsole** draait helemaal zonder grafische bedieningsinterface en heeft verder geen parameters voor de weergave nodig.

De wlan-scanner **inSSiDer 2** is op .NET gebaseerd en werkt daarmee ook op Vista en Windows 7. De resultaten worden in grafieken gezet om bijvoorbeeld overbevolkte wlan-frequenties te vinden. Het programma registreert met de bijbehorende gps-accessoires eveneens de geodata van de actieve wlan-basisstations, wat helpt bij het plannen van grote draadloze netwerken.

## Bezorgservice

Als je Windows-pc's zonder extra router in een netwerk wilt opnemen, ontbreekt vaak een makkelijk te configureren DHCP- en DNS-server en een kleine server voor HTTP en remote access.

Daar springt het opensource en vrij te configureren **Tftpd32** op in. Het programma heeft DHCP-, DNS- en TFTP-server en een client voor TFTP samen in één grafische interface, zodat je de betreffende computer ook als remote-bootserver kunt gebruiken. Tftpd32 verzamelt bovendien systeemmeldingen via syslog en ondersteunt IPv6.

Als een pc snel een aantal bestanden aan andere computers in hetzelfde netwerk moet afleveren, gaat dat meestal sneller via een kleine webserver. De 560 kB grote **HTTP File Server** (HFS) draait ook vanaf een usb-stick en slaat zijn instellingen zonodig daar ook op. De inhoud van mappen en bestanden wordt via HTTP getoond. De toegang tot deze shares kan tot bepaalde gebruikers worden beperkt of uitgebreid – inclusief schrijfrechten en snelheidslimieten. Je kunt de standaard weergavesjablonen aan je eigen smaak aanpassen.

**MobaSSH** voegt een OpenSSH-server aan Windows toe, die bij de start een systeemservice wordt. De eenvoudige bediening via de tekstconsole verbruikt in tegenstelling tot Remote Desktop slechts weinig dataverkeer. SSH-clients als **PuTTY** of **kiTTY** zijn geschikt voor een betrouwbare toegang tot de MobaSSH-tekstconsole. Omdat MobaSSH gebaseerd is op OpenSSH, kan hij ook TCP-verbindingen (bijvoorbeeld VNC) door de versleutelde SSH-tunnel sturen en VPN's opbouwen. MobaSSH heeft eigen editors voor opties die niet via de bedieningsinterface ingesteld kunnen worden. Hiermee kunnen de centrale SSH-configuratie, het aanmeldprofiel en andere instellingen direct bewerkt worden. MobaSSH levert via het bij SSH horende SFTP ook bestanden aan programma's als **WinSCP**, wat aan te raden is bij een overdracht via internet.

## Hulp op afstand

Om een grafische gebruikersinterface op afstand te bedienen, heb je op de betreffende computer een VNC-server nodig als **TightVNC** en op je eigen pc een VNC-client. De populaire Windows-VNC-server **UltraVNC** heeft een Windows-VNC-client. Als bescherming tegen afluisteren wordt de VNC-verbinding via een versleutelde SSH-tunnel (TCP-forwarding) geleid. Als de te bedienen computer achter een NAT-router staat, moet die de SSH-poort doorsturen naar het lokale netwerk. SSH en VNC zijn daarom minder geschikt om iemand snel even via internet te helpen.

Tools als **Teamviewer** gaan meestal moeiteloos over netwerkgrenzen heen en kunnen twee kanten op werken. Teamviewer draait zonder installatie en zelfs videotelefonie is er mee mogelijk. (nkr) c't


**MobaSSH breidt Windows-computers uit met een OpenSSH-server, waarmee bestanden veilig kunnen worden overgedragen en kan bovendien gebruikt worden voor het beveiligen van onversleutelde diensten als VNC.**