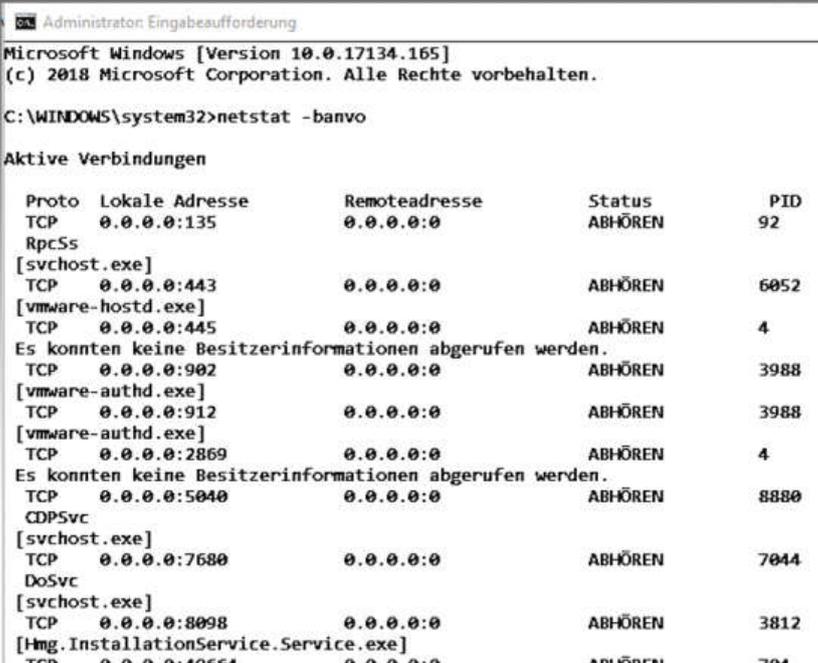




In vielen Haushalten kommt eine Fritz!Box zum Einsatz. In der Weboberfläche der [Fritzbox](#) erhalten Sie Informationen zu den einzelnen Geräten, die im Netzwerk vorhanden sind. Rufen Sie dazu die Oberfläche mit <https://fritz.box> auf, und melden Sie sich mit dem Kennwort an, das auf der Rückseite der Fritzbox steht; oder das Sie selbst gesetzt haben. Den wichtigsten Überblick erhalten Sie über Heimnetz/Heimnetzübersicht. Hier sehen Sie die verschiedenen Geräte im Netzwerk, und welche Endgeräte aktuell eine Verbindung aufgebaut haben. Über den Link Heimnetz/Netzwerk sehen Sie wiederum alle aktuellen Endgeräte. Überprüfen Sie an dieser Stelle, ob es Geräte gibt, die im [Netzwerk](#) nichts zu suchen haben. Sie können die Informationen an dieser Stelle auch für Tools nutzen, die wir Ihnen in diesem Beitrag ebenfalls vorstellen.

## Geöffnete Netzwerk-Ports auf Viren und Trojaner überprüfen

Ein PC kommuniziert über seine IP-Adresse über den Router, also zum Beispiel einer [Fritzbox](#), mit dem Internet. Dabei nutzen verschiedene Programme unterschiedliche Netzwerk-Ports der IP-Adresse, die dem Router vom Provider zugewiesen wurde. In der Befehlszeile von Windows können Sie überprüfen, welche Ihrer Programme eine Verbindung zum Internet aufbauen und welche Ports genutzt werden. So lassen sich auch Viren und Trojaner erkennen. Wenn Sie bestimmte Programme nicht identifizieren können, suchen Sie nach dem Namen im Internet. In den meisten Fällen finden Sie recht schnell Informationen zu allen Programmen.



```
Administrator Eingabeaufforderung
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>netstat -banvo

Aktive Verbindungen

Proto Lokale Adresse Remoteadresse Status PID
TCP 0.0.0.0:135 0.0.0.0:0 ABHÖREN 92
RpcSs
[svchost.exe]
TCP 0.0.0.0:443 0.0.0.0:0 ABHÖREN 6052
[vmware-hostd.exe]
TCP 0.0.0.0:445 0.0.0.0:0 ABHÖREN 4
Es konnten keine Besitzerinformationen abgerufen werden.
TCP 0.0.0.0:902 0.0.0.0:0 ABHÖREN 3988
[vmware-authd.exe]
TCP 0.0.0.0:912 0.0.0.0:0 ABHÖREN 3988
[vmware-authd.exe]
TCP 0.0.0.0:2869 0.0.0.0:0 ABHÖREN 4
Es konnten keine Besitzerinformationen abgerufen werden.
TCP 0.0.0.0:5040 0.0.0.0:0 ABHÖREN 8880
CDPSvc
[svchost.exe]
TCP 0.0.0.0:7680 0.0.0.0:0 ABHÖREN 7044
DoSvc
[svchost.exe]
TCP 0.0.0.0:8098 0.0.0.0:0 ABHÖREN 3812
[Hmg.InstallationService.Service.exe]
TCP 0.0.0.0:40664 0.0.0.0:0 ABHÖREN 704
```

© PC Magazin

Mit dem Bordmittel netstat lassen sich Netzwerkinformationen anzeigen.

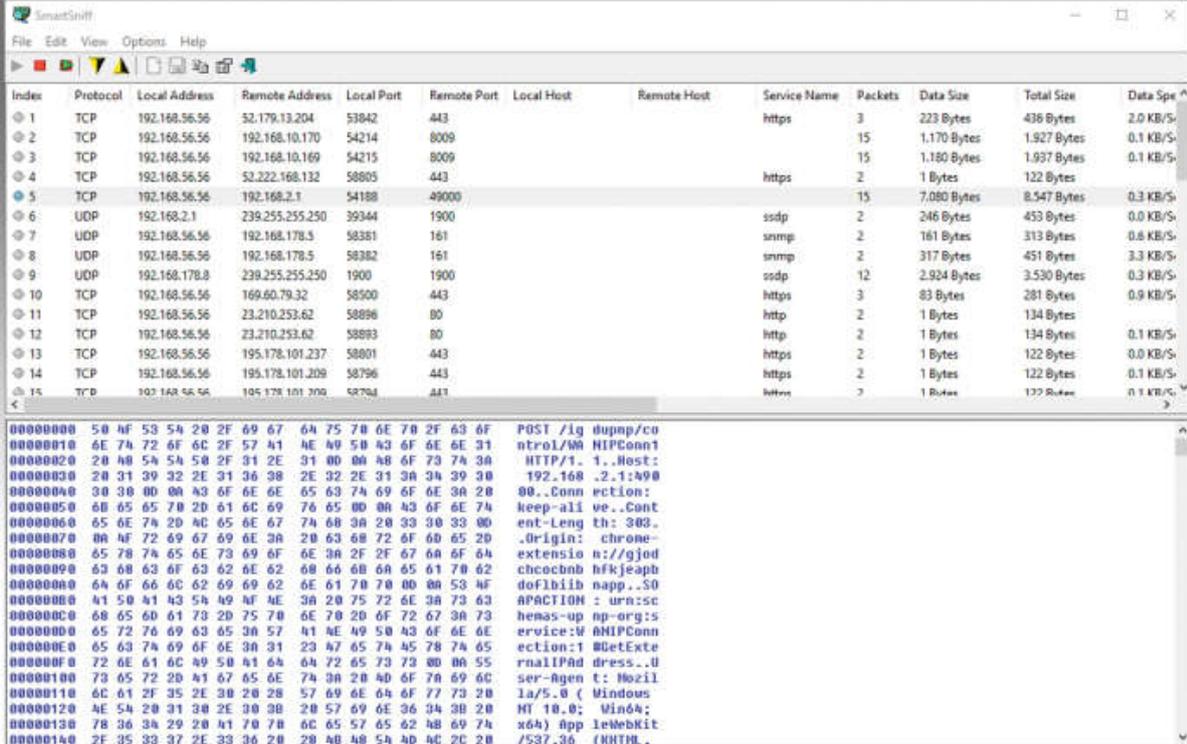
Geben Sie in der Befehlszeile den Befehl netstat -an ein, zeigt Windows die geöffneten Ports. Ausführlichere Informationen erscheinen mit netstat -banvo. Die Routingtabelle des Computers wird mit netstat -r angezeigt, Statistiken zu TCP/IP sehen Sie mit netstat -san. So lassen sich umfassende Informationen zu den Netzwerkeinstellungen eines Computers abrufen.

Sysinternals liefert mit [TCPView](#) ein einfaches Programm, mit dem auch unerfahrene Anwender erkennen, welche Netzwerkverbindungen aktuell geöffnet sind. Der Softwareentwickler NirSoft stellt ein ähnliches kostenloses Tool mit der Bezeichnung [CurrPorts](#) zur Verfügung. Wie TCPView muss auch das Gratis-Tool CurrPorts nicht installiert werden.

## Kostenlose Analyse-Tools

[SmartSniff](#) ist ein kleines Tool, um Netzwerkverbindungen auf einem [Computer](#) zu erkennen. Das Tool lässt sich direkt und ohne Installation starten. Auch Einsteiger in die Netzwelt kommen daher schnell damit zurecht.

## Anzeige



The screenshot shows the SmartSniff application interface. The top part is a table with columns: Index, Protocol, Local Address, Remote Address, Local Port, Remote Port, Local Host, Remote Host, Service Name, Packets, Data Size, Total Size, and Data Sp... Below the table is a hex dump of captured data, showing hexadecimal values and their corresponding ASCII characters.

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host	Service Name	Packets	Data Size	Total Size	Data Sp...
1	TCP	192.168.56.56	52.179.132.204	53842	443			https	3	223 Bytes	438 Bytes	2.0 KB/S
2	TCP	192.168.56.56	192.168.10.170	54214	8009				15	1.170 Bytes	1.927 Bytes	0.1 KB/S
3	TCP	192.168.56.56	192.168.10.169	54215	8009				15	1.180 Bytes	1.937 Bytes	0.1 KB/S
4	TCP	192.168.56.56	52.222.168.132	58805	443			https	2	1 Bytes	122 Bytes	
5	TCP	192.168.56.56	192.168.2.1	54188	49000				15	7.080 Bytes	8.547 Bytes	0.3 KB/S
6	UDP	192.168.2.1	239.255.255.250	39344	1900			ssdp	2	246 Bytes	453 Bytes	0.0 KB/S
7	UDP	192.168.56.56	192.168.178.5	58381	161			snmp	2	161 Bytes	313 Bytes	0.6 KB/S
8	UDP	192.168.56.56	192.168.178.5	58382	161			snmp	2	317 Bytes	451 Bytes	3.3 KB/S
9	UDP	192.168.178.8	239.255.255.250	1900	1900			ssdp	12	2.924 Bytes	3.530 Bytes	0.3 KB/S
10	TCP	192.168.56.56	169.60.79.32	58500	443			https	3	83 Bytes	281 Bytes	0.9 KB/S
11	TCP	192.168.56.56	23.210.253.62	58898	80			http	2	1 Bytes	134 Bytes	
12	TCP	192.168.56.56	23.210.253.62	58893	80			http	2	1 Bytes	134 Bytes	0.1 KB/S
13	TCP	192.168.56.56	195.178.101.237	58801	443			https	2	1 Bytes	122 Bytes	0.0 KB/S
14	TCP	192.168.56.56	195.178.101.209	58796	443			https	2	1 Bytes	122 Bytes	0.1 KB/S
15	TCP	192.168.56.56	195.178.101.200	58794	443			https	2	1 Bytes	122 Bytes	0.1 KB/S

```
00000000 50 4f 53 54 20 2f 69 67 64 75 70 6e 78 2f 63 6f POST /ig dupmp/co
00000001 6e 74 72 6f 6c 2f 57 41 4e 49 50 43 6f 6e 6e 31 ntrol/WIPConn1
00000002 20 48 54 54 50 2f 31 2e 31 00 00 48 6f 73 74 30 HTTP/1.1..Host:
00000003 20 31 39 32 2e 31 36 38 2e 32 2e 31 3a 3a 39 30 192.168 .2.1:490
00000004 30 30 00 00 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 00..Conn ection:
00000005 60 65 65 70 20 61 6c 69 76 65 00 00 43 6f 6e 74 keep-ali ve..Cont
00000006 65 6e 74 20 4c 65 6e 67 74 68 3a 20 33 30 33 00 ent-Leng th: 303.
00000007 0a 4f 72 69 67 69 6e 3a 20 63 68 72 6f 60 65 20 .Origin: chrone-
00000008 65 78 74 65 6e 73 69 6f 6e 3a 2f 2f 67 6a 6f 64 extensio n://gjed
00000009 63 68 63 6f 63 62 6e 62 68 66 68 6a 65 61 70 62 chcobnb hfkjeaph
0000000a 64 6f 66 6c 62 69 69 62 6e 61 70 70 00 0a 53 4f dof1biib napp..50
0000000b 41 50 41 43 54 49 4f 4e 3a 20 75 72 6e 3a 73 63 APACTIION : urn:sc
0000000c 68 65 60 61 73 20 75 70 6e 70 20 6f 72 67 3a 73 hemas-up np-org:s
0000000d 65 72 76 69 63 65 30 57 41 4e 49 50 43 6f 6e 6e ervice:W IPIPConn
0000000e 65 63 74 69 6f 6e 3a 31 23 47 65 74 45 78 74 65 ction:1 00etExte
0000000f 72 6e 61 6c 49 50 41 64 64 72 65 73 73 00 0a 55 rnalIPad dress..U
00000010 73 65 72 20 41 67 65 6e 74 3a 20 40 6f 7a 69 6c ser-Agen t: Mozil
00000011 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 ( Windows
00000012 4e 54 20 31 3a 2e 30 30 20 57 69 6e 36 34 20 20 NT 10.0; Win64;
00000013 78 36 3a 29 20 41 70 70 6c 65 57 65 62 48 69 74 x64) App leWebKit
00000014 2f 35 33 37 2e 33 36 20 20 4b 48 54 40 4c 2c 20 /537.36 (KHTML,
```

© PC Magazin

SmartSniff hilft bei der Analyse des Netzwerkverkehrs.

Nach dem Start beginnt der Vorgang mit einem Klick auf das grüne Dreieck, um den Untersuchungsvorgang zu starten. Anschließend zeigt das Tool die Verbindungen des Computers im [Netzwerk](#) und ins Internet an. Im Fenster sind dann das Protokoll, die lokale Adresse, die Remoteadresse, der Port, der Name des Dienstes, die Größe des Datenpakets und die Geschwindigkeit zu sehen. Durch einen Klick auf die Verbindung sehen Sie im unteren Bereich weitere Informationen. Geben Sie die Daten in einer Suchmaschine ein, erhalten Sie weitere Informationen zum entsprechenden Bereich. So erkennen Sie schnell einen verdächtigen oder nicht gewollten Netzwerkverkehr.

## Wireshark: Gratis Netzwerkanalyse

Geht es um die Analyse von Netzwerken, gehört die Opensource-Lösung [Wireshark](#) zu den bekanntesten Lösungen. Nach dem Start stehen viele Optionen zur Verfügung. In der Titelleiste sind Informationen zu den aktuellen Scanvorgängen zu sehen und die Version von Wireshark. Das Scannen des Netzwerks erfolgt in einer grafischen Oberfläche. Sobald der Scanvorgang gestartet ist, zeigt Wireshark im Fenster Informationen an. Die Optionen der Scanvorgänge zeigt das Tool in der grafischen Oberfläche über Aufzeichnen/Optionen an. Nach dem Start erfolgt die Aufnahme, indem Sie auf den Menüpunkt Aufzeichnung von Paketen starten klicken.

## NetworkTrafficView scannt ebenfalls aktive Netzwerke

Haben Sie mit SmartSniff das [Netzwerk](#) im Blick, können Sie vom gleichen Entwickler das Tool [NetworkTrafficView](#) einsetzen. Das Tool zeigt von lokalen Rechnern aus an, welche Pakete von Quell- zu Ziel-Adressen geschickt werden. NetworkTrafficView weist auch auf das lokale Programm hin, welches die Daten versendet sowie den Quell- und Ziel-Port. Wenn möglich, wird auch das Icon des entsprechenden

Programmes angezeigt. Mit NetworkTrafficView sehen Sie aber auch Pakete, die von anderen Rechnern im Netzwerk gesendet werden.

Im Gegensatz zu SmartSniff zeigt NetworkTrafficView aber nicht den Inhalt der Pakete an, sondern nur deren Quell- und Ziel-Daten. Markieren Sie einen Prozess, können Sie sich über File/Properties noch mehr Informationen über das Paket anzeigen lassen. Sie sehen im Fenster zusätzlich noch den Zeitpunkt des Sendevorgangs, die verantwortlichen Prozesse und die Größe der Pakete. Über das Kontextmenü einzelner Pakete können Sie diese speichern und als Mail versenden, wenn Sie zum Beispiel mehr Informationen benötigen. In der Praxisanwendung und vielen Tests zeigte sich, dass das Tool gut mit SmartSniff zusammenarbeitet.

## Scan per Antivirenprogramm und Smartphone



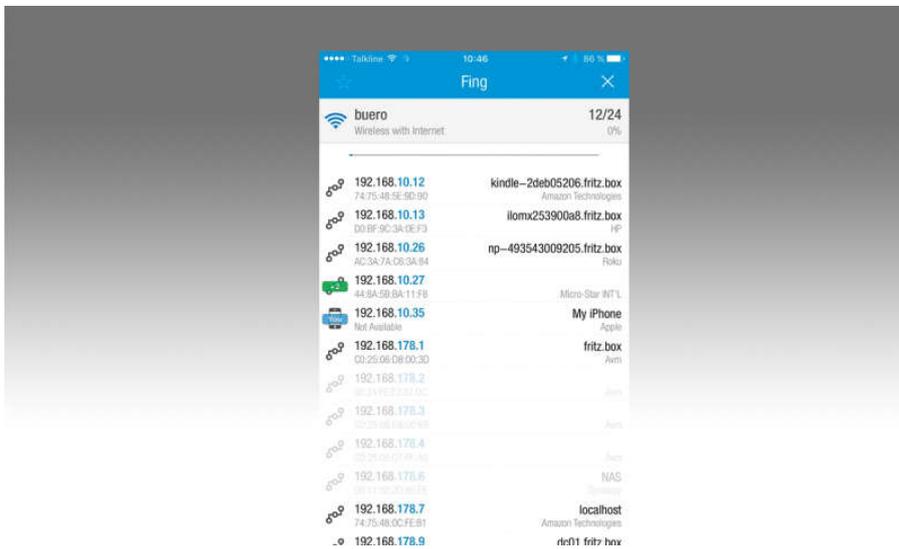
© PC Magazin

Virens Scanner wie Avast zeigen Schwachstellen im WLAN an.

Viele Virens Scanner, zum Beispiel der kostenlose [Virens Scanner Avast Free Antivirus](#), verfügen über einen zusätzlichen Schutz, der das Netzwerk nach Sicherheitslücken durchsucht. Betreiben Sie Avast Free Antivirus, kann das Tool dabei helfen, den Netzwerkschutz zu verbessern. Dazu rufen Sie die Verwaltungsoberfläche des Tools auf und wählen bei Schutz die Option WLAN-Inspektor. Hier erhalten Sie Informationen zu den Geräten und den Problemen im Netzwerk. Ähnliche Optionen bieten auch viele andere kostenlose Scanner. Sie sollten in der Anleitung oder Hilfe überprüfen, ob Ihr [Virens Scanner](#) über eine solche Funktion verfügt und diese regelmäßig aufrufen.

## Mit Smartphone auf Schwachstellensuche

Mit der kostenlosen App Fing ([iOS](#), [Android](#)) lassen sich Netzwerke mit dem Smartphone untersuchen, Inventare erstellen und Sicherheitslücken finden. Darüber hinaus kann die kostenlose App auch die offenen Ports und andere Informationen von Netzwerkgeräten auslesen und Informationen anzeigen.

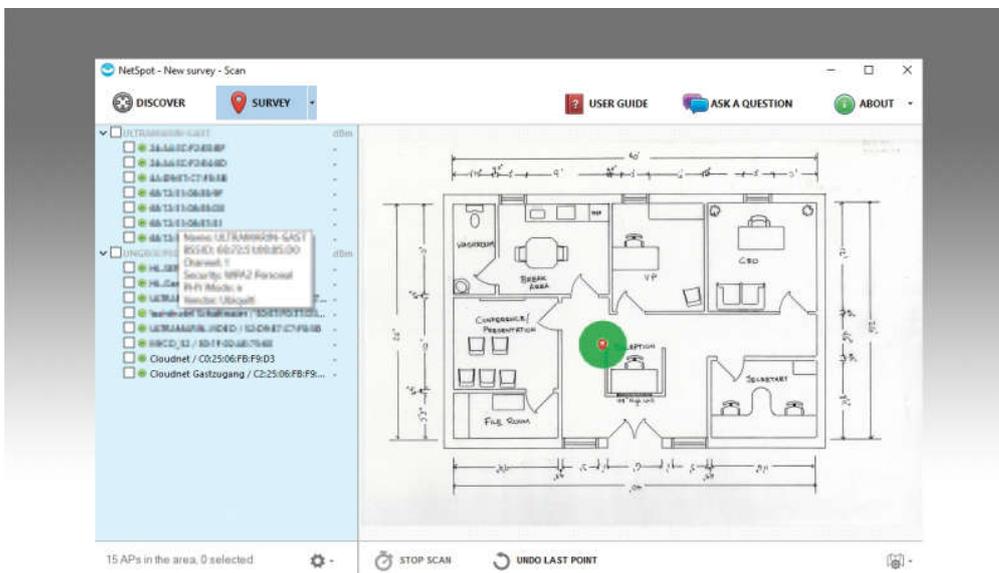


© PC Magazin

Die App Fing kann auf dem Smartphone WLANs testen.

Eine interessante Alternative zu Fing ist die App [Network Ping Lite](#) für Apple-Geräte. Auch mit dieser App lassen sich Netzwerke auf aktiven [Geräte](#) scannen und Daten auswerten. Sicherheitslücken werden hier ebenso schnell erkannt.

## NetSpot beschleunigt WLAN, SmartSniff verfolgt Online-Traffic



© PC Magazin

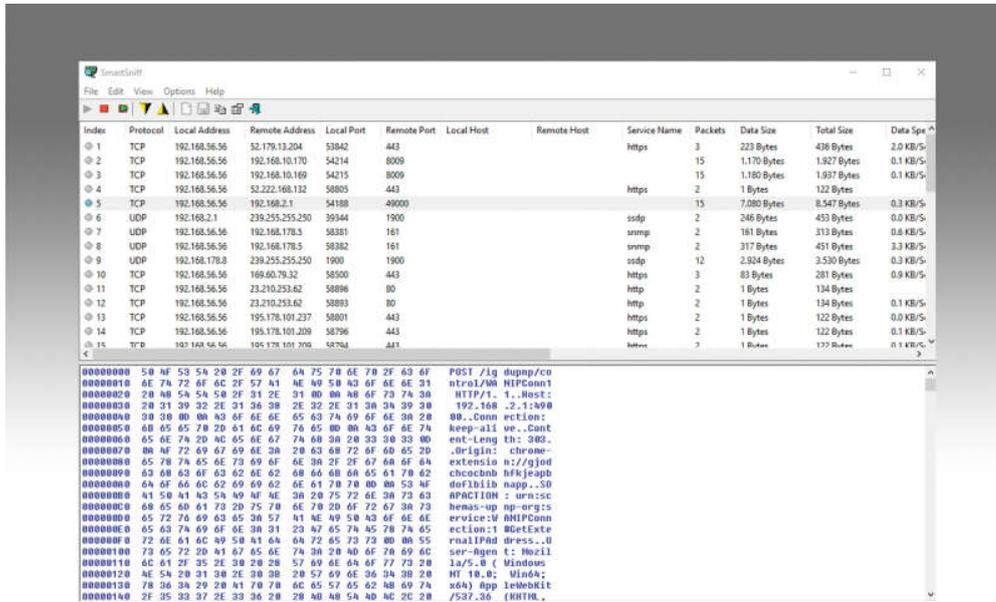
NetSpot hilft dabei, WLAN-Geräte optimal im Haus zu positionieren und tote Winkel zu vermeiden. Anzeige

Mit dem Tool [NetSpot](#), das für macOS X und [Windows](#) zur Verfügung steht, können Sie die Verfügbarkeit und Leistung von WLANs überprüfen. Nachdem das Tool installiert ist, überprüft es die Verfügbarkeit der WLANs im Gebäude. Der Vorteil von NetSpot liegt darin, dass auch Anwender oder Administratoren ohne umfassende Kenntnisse von einer Netzwerkanalyse schnell und einfach einen Überblick zu den einzelnen WLANs erhalten. Sobald das Tool gestartet ist, zeigt es alle verfügbaren WLANs sowie deren Signalstärke an. So lassen sich

Probleme bei Netzwerkverbindungen und Fehlkonfigurationen sehr schnell finden, ohne komplizierte oder komplexe Konfigurationen vornehmen zu müssen.

Neben der optimalen Positionierung von WLAN-Geräten, ist das Tool natürlich auch auf [Notebooks](#) sinnvoll, die sich in der Regel auf Grund der mobilen Nutzung an unterschiedlichen Standorten mit verschiedenen WLANs verbinden. Denn durch wenige Klicks ist zu sehen, welche WLANs optimal verbunden werden können und wo es Probleme bei der Reichweite und dann auch letztlich mit einer stabilen Verbindung für Datentransfers gibt.

## Pakete im Internet mit Gratis-Online-Tools nachverfolgen



© PC Magazin

SmartSniff hilft bei der Analyse des Netzwerkverkehrs.

Haben Sie mit SmartSniff Datenpakete entdeckt, die ins Internet versendet werden, zeigt das Tool entweder den Namen des Servers an oder nur die IP-Adresse, wenn der Name nicht aufgelöst werden kann. Sie haben in diesem Fall auch die Möglichkeit, den Weg des Paketes anzuzeigen und den Namen des Servers im Internet herauszufinden. Auf der Seite [Network-Tools.com](#) können Sie IP-Adressen effizient nach Servernamen auflösen und einen Trace-Vorgang, also eine Ablaufverfolgung, für die Pakete durchführen.