## So testen Sie Ihr Heimnetz auf Schwachstellen

16.10.2018

#### Inhalt

- 1. Netzwerk-Sicherheit: So testen Sie Ihr Heimnetz auf Schwachstellen
- 2. <u>Netzwerk-Sicherheit: Kostenlose Analyse-Tools</u>
- 3. Netzwerk-Sicherheit: Scan per Antivirenprogramm und Smartphone
- 4. Netzwerk: NetSport beschleunigt WLAN, SmartSniff verfolgt Online-Traffic



<u>Netzwerk</u>. Sobald eine Verbindung zum Internet aufgebaut wird und PCs, Notebooks, Smartphones und Tablets zum Einsatz kommen, sind diese miteinander vernetzt. In Unternehmen kümmert sich die IT-Abteilung um die Sicherheit. In Privathaushalten sorgen Sie für Sicherheit und Überblick. Dazu liefern wir in diesem Artikel verschiedene Hilfsmittel und Tools.

## Überblick in der Fritzbox-Oberfläche

leimnetz > Heimnetzüb	versicht		
eimnetz und WLAN Mesh			ି ସେଖିକ ଏସେରାMbd//aiPhone
FRITZIBox 7590 IP-Adresse: 192.168.2.1	🖞 LANI 91.058/s	PC-192-168-180-21	
WLAN-Funknetz	ETZ A LAN 1 +1 CORIN	PC-192-168-10-146 IP-Adresser 152.168.10.146	
TV	A LANI HIGHRA	PC-192-168-178-1 IF-Adresse: 152.168.178.1	nas
	#a UAN 1 →1 Gbit/a	Android-2 19-Adresser 392.168.10.124	

Die Weboberfläche der Fritz!Box zeigt angebundene Geräte.

In vielen Haushalten kommt eine Fritz!Box zum Einsatz. In der Weboberfläche der <u>Fritzbox</u> 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 <u>Netzwerk</u> 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 <u>Fritzbox</u>, 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	E.			
Microsoft Windows [Version (c) 2018 Microsoft Corporat				
C:\WINDOW5\system32>netstat	-banvo			
Aktive Verbindungen				
Proto Lokale Adresse	Remoteadresse	Status	PID	
TCP 0.0.0:135	0.0.0.0:0	ABHÖREN	92	
<pre>kpcSs [sychost.exe]</pre>				
TCP 0.0.0.0:443	0.0.0.0:0	ABHÖREN	6052	
[vmware-hostd.exe]	0 0 0 0 0	ADUSDEN		
Es konnten keine Resitzeri	0.0.0.0:0	ABHOKEN	4	
TCP 0.0.0.0:902	0.0.0.0:0	ABHÖREN	3988	
[vmware-authd.exe]				
TCP 0.0.0:912	0.0.0.0:0	ABHÖREN	3988	
[vmware-authd.exe]		ADLIGOCAL		
Es konnten keine Resitzeri	nformationen abgerufen	ABHUKEN	4	
TCP 0.0.0.5040	0.0.0.0:0	ABHÖREN	8880	
CDPSvc				
[svchost.exe]			100000000	
TCP 0.0.0.0:7680	0.0.0.0:0	ABHOREN	7044	
[sychost_exe]				
TCP 0.0.0:8098	0.0.0.0:0	ABHÖREN	3812	
[Hmg.InstallationService.S	ervice.exe]			
TOD A A A A AGEA	A A A A A	ARHÖREN	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 <u>TCPView</u> 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 <u>CurrPorts</u> zur Verfügung. Wie TCPView muss auch das Gratis-ToolCurrPorts nicht installiert werden.

## **Kostenlose Analyse-Tools**

<u>SmartSniff</u> ist ein kleines Tool, um Netzwerkverbindungen auf einem <u>Computer</u> zu erkennen. Das Tool lässt sich direkt und ohne Installation starten. Auch Einsteiger in die Netzwelt kommen daher schnell damit zurecht.

Anzeige

Carrier Server	tSniff										-	ц×
File Edi	t View C	ptions Help										-
▶ <b>■</b> 1	• <b>7</b> <u>A</u>	口口回题或	1 <b>- 1</b>									
Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host	Service Name	Packets	Data Size	Total Size	Data Spe ^
0.1	TCP	192,168.56.56	52.179.13.204	53842	443			https	3	223 Bytes	436 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
03	TCP	192.168.56.56	192,168,10,169	54215	8009				15	1.150 Bytes	1.937 Bytes	0.1 KB/5-
04	TCP	192,168,56,56	52,222,168,132	58805	443			https	2	1 Bytes	122 Bytes	10000
0.5	TCP	192,168,56,56	192,168,2,1	54188	49000			20	15	7.080 Bytes	8.547 Bytes	0.3 KB/S
0.6	UDP	192,168,2,1	239,255,255,250	10744	1900			estin	2	246 Bytes	453 Butet	0.0 KB/S
07	LIDE	192 168 56 56	192 168 178 5	58281	161			Sector .	3	161 Butes	313 Butes	DAKE/S.
0.8	LIDP	107 168 56 56	102 168 179 5	59383	141			and the second se	3	317 Buter	JS1 Buter	23 KE/S.
0.0	LIDD	103 168 179 8	330 355 355 350	1000	1900			and a	12	2 924 Puter	3 530 Buter	0.2 /8/5
-0.10	TCP	102 160 170.0	160 60 70 37	techn	A42			and p	3	23 Dutor	301 P. 444	OG KB/S
0.11	TCD	101 149 55 55	10 210 252 67	Eagle	00			hinter .	-	1 Bates	131 Butes	Mar NB/ 31
0.11	TCD	192,100,30,20	23/210/233/02	20020	00			http	2	1 Bytes	134 Dytes	0.1 10.0
0.12	TCP	192,108,30,36	23.210.233.02	20075	445			intp	-	1 bytes	134 Bytes	OLT KB/S
0 13	ICP	192.108.30.36	195.178.101.237	36801	943			inttps	-	1 Bytes	122 Bytes	0.0 KB/S
14	ICP	192.168.96.96	195.178.101.209	38,796	443			https	4	1 Bytes	122 Bytes	0.1 KB/S-
< 15	TCP	42 42 841 CDI	195 178 101 209	68764	AI1			Buttone		1 Butes	132 Sufee	AT KR/6.*
0000000	10 50 40	53 54 28 21	69 67 64 75	5 78 6E 78	2F 63 6F	POST /ig dupmp/	/c0					•
0000001	@ 6E 74	4 72 6F 6C 2	57 41 4E 41	50 43 6F	6E 6E 31	ntrol/WA NIPCon	101					100
00088982	0 28 4	1 20 22 25 2	1 34 39 3F 31	2 2E 31 36	20 20 20	102 168 2 1-1	0.0					
8868888	0 30 31	8 00 0A A3 A	F 6E 6E 65 65	74 69 6F	6E 38 28	80. Conn ection						
0000005	0 60 65	5 65 78 20 6	1 60 69 76 65	00 0A 43	6F 6E 74	keep-ali veCo	ant					
0000000	0 65 60	E 74 20 40 65	5 6E 67 74 64	3 34 28 33	38 33 80	ent-Leng th: 30	. 33					
00008807	0 88 4	72 69 67 6	9 6E 3A 20 65	68 72 6F	60 65 20	.Origin: chron	he -					
	0 65 /1	8 74 05 OE 7	3 0 9 0F 0E 36	AB 40 45	OH OF 04	excensio n://g)	00					
0000000	10 6h 6i	F 66 6C 62 6	0 69 62 6F 61	78 78 80	88 53 45	doflbiib nann.	50					
1000000	41 51	0 41 43 54 44	AF 4E 36 20	3 75 72 6E	38 73 63	APACTION : urn:	50					
0000000	0 68 65	5 60 61 73 2	0 75 70 6E 70	0 20 6F 72	67 3A 73	hemas-up np-org	115					
1000000	0 65 73	2 76 69 63 6	5 30 57 41 4	49 50 43	OF GE GE	ervice:W ANIPCo	nne					
00008888	0 65 63	1 74 09 6F 6	E 30 31 23 4/	65 74 45	78 74 65	ection:1 BGetEx	tte					
00888914	10 73 6	5 72 20 A1 A	7 65 6E 7h 30	28 40 AF	78 69 60	ser-Agen t: Mag	ii					
0008011	0 36 8	1 2F 35 2E 3	0 20 28 57 65	6E 64 6F	77 73 20	la/5.0 ( Window	15					
0000012	10 4E 54	4 28 31 38 21	E 30 38 20 57	69 6E 36	34 38 28	HT 18.0; Win64	12					
8888013	10 78 30	5 34 29 28 4	1 70 70 60 65	57 65 62	48 69 74	x64) App leWebH	lit					
0000011	B 9E 98		1 TAA TEAL 7151 A.S.		P	AND THE ADDRESS OF MANY SAME						

#### © 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 <u>Netzwerk</u> 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 <u>Wireshark</u> 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 <u>Netzwerk</u> im Blick, können Sie vom gleichen Entwickler das Tool <u>NetworkTrafficeView</u> 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

	Schutz > WLAN-Inspektor		
Status	WLAN-Inspektor 💿		Kartenansicht Listenansicht
₿	Sieht gut aus! Keine	Probleme in diesem Ne Netzwerkname: 🖱 Mitz.box 🛈	tzwerk gefunden.
Schutz		Netzwerkname: fritz.box	
		IP-Adresse: 79.213.132.125	
Privatsphäre		Standort. 74245, Loewenstein,	
		Germany, Europe Internetdienstanbieter:	
Leistung		Deutsche Telekom AG	
century			
AKTIVIEREN		í — — — — i	

© PC Magazin

Virenscanner wie Avast zeigen Schwachstellen im WLAN an.

Viele Virenscanner, zum Beispiel der kostenlose <u>Virenscanner Avast Free Antivirus</u>, 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 <u>Virenscanner</u> über eine solche Funktion verfügt und diese regelmäßig aufrufen.

### Mit Smartphone auf Schwachstellensuche

Mit der kostenlosen App Fing (<u>iOS</u>, <u>Android</u>) 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.

	- Labeline 🗢	Fing	×
(	buero Wireless with Internet		12/24 0%
50 <sup>9</sup>	<b>192.168.10.12</b> 74.75.48.55.90.90	kindle-2de	b05206.fritz.box
508	192.168.10.13 D0 BF 9C 3A 0E F3	ilomx25	3900a8.fritz.box
50 <sup>9</sup>	192.168.10.26 AC 34 74 CB 34 84	np-493543	009205.fritz.box
<b>6</b>	192.168.10.27 44:8A:58:8A:11:F8		Micro-Star INT'L
	192.168.10.35 Not Available		My iPhone Apple
60 <sup>9</sup>	192.168.178.1 00 25 06 08:00:30		fritz.box
509	192.168.178.2		
509	192.168.178.3		
502	192.168.178.4		
509	192.168.178.6		NAS
50 <sup>9</sup>	192.168.178.7	3	localhost
.0	192.168.178.9		dc01 fritz box

© PC Magazin

Die App Fing kann auf dem Smartphone WLANs testen.

Eine interessante Alternative zu Fing ist die App <u>Network Ping Lite</u> für Apple-Geräte. Auch mit dieser App lassen sich Netzwerke auf aktiven <u>Geräte</u> scannen und Daten auswerten. Sicherheitslücken werden hier ebenso schnell erkannt.

# NetSport 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 <u>NetSpot</u>, das für macOS X und <u>Windows</u> 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 <u>Notebooks</u> 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

W Lorent	Snitt																					<u>2</u>	ш×
Die Lin	View	-	in all	i la	2																		
		A	D1	III s	7 54 195		1																
Index	Protoco	-	local	Add		2,	mote	Add	interio	Loc	al Po		Ren	- No P	inter a	Local Heat		Remote Host	Service Name	Backets	Data Site	Total Gra	Data See 1
0.1	TOP		107 1			57	170.1	2 20		530	12		412						hitter	1	222 Buter	476 D. fee	20 KB/S
0.2	TCD		192.1	10 EE	56	10	0 168	10.1		5.83	14			ŝ					ringes	15	1170 Puter	1.927 D.dar	0.1 KE/S
	TCD		192.1	00.30.	20	32	2.100.	10.1	10	200			000	<u>.</u>						12	1.170 Bytes	1.927 Bytes	0.1 KB/3
	TCP		192.1	00.30.	2	19	2,100.	100.10		244	12		0.0						10000 C	13	1. Tou bytes	1.957 Bytes	U.1 KD/3-
	TCP		122.1	10.20.		20	222.0	3.0	26	100	10		450						mupS	15	7 OPD B. Aver	D S ST D Sec	DIVER
	LIDD		192.1	00.20.	10	19	C-100.	100	160	241	14		100						200402	2	7.000 Bytes	6.34/ Bytes	O O KE/SI
	UDP		192.1	00.2.1		23	3,233,	170	230	293			190						ssap	-	240 bytes	ass dytes	ULD KB/S
91	UDP		192.10	08.36.	20	19	2.165.	178.	2	583	51		101						munt	2	161 Bytes	313 Bytes	0.6 KB/S+
	UDP		192.1	06.30.	90	19	2.108.	1/8.3	2	563	K		101						smmp	*	317 Bytes	451 Bytes	3.3 KB/5-
0.8	UDP		192.1	58.174	8.1	-23	9.255.	200.4	250	190			190						sedp	12	2.924 Bytes	3.530 Bytes	0.3 KB/S
@ 10	TCP		192.1	68.56.	50	16	9.60.7	9.32	3	585	00		443						Pettges	3	83 Bytes	281 Bytes	0.9 KB/S-
0.11	TCP		192.1	68.56	20	23	210.2	53.6	2	588	36		90						http	2	1 Bytes	134 Bytes	1000
··· 12	TCP		192.14	08.56.	20	23	210.2	33.6	2	588	83		80						nttp	2	1 Bytes	134 Bytes	0.1 KB/Sr
0 13	ICP		192.1	08.50	00	19	5.178.	101.	131	M	0		- 443						https	2	1 Bytes	122 Bytes	0.0 KB/S
@ 14	TCP		192.10	68.56.	56	19	5.178	101.3	209	587	90		443						https	2	1 Bytes	122 Bytes	0.1 KE/S-
< 15	308		103.1	63.56	200	19	5 178	101	ma	683	9.00		A						Internet		1 Botes	132 Suter	3
0000000	0 50	ħF	53	54 2	0 2	61	67	6	4 7	5 71	6E	70	2F	63 6	F	POST /1	9 9	lupnp/co					
00000000	8 OL	74	72	6F 6	6 21		41	4	1 01	5	43	OF AE	0L.	6L 3	1	ntrol/w	٩.	IPConn1					
0000883	0 20	31	39	32 2	E 3	1 31	\$ 38	2	E 3	2 28	31	SA	34	39 3		192.16	8.	2.1:498					
8088804	8 38	38	00	6A 4	3 61	6	E 6E	6	5 61	1 71	69	6F	6E	3A 2		88Con		ction:					
0009995	0 60	65	65	78 2	DÓ	1 61	: 69	7	6 6	00	BA	43	6F	6E 7	4	keep-al	1.1	eCont					
00000000	0 8	10	79	20 4	0 0	0	1 90		4 01	3 31	20	33	38	33 8		ent-Len	9.1	n: 303.					
00000007	8 65	78	78	65 6	E 7	6 61	6F	6	E 34	1 26	21	67	68	6F 6	4	extensi	ñ 1	://nind					
0000009	6 63	68	63	6F 6	3 61	2 61	62	ő	8 64	5 68	6A	65	61	70 6	2	chcocbn	6 1	fkjeapb					
0000000	0 64	6F	66	60 6	2 61	61	1 62	6	E 61	1 71	70	80	BA	53 4	F	doflbii	b r	appS0					
00000000	8 41	50	41	43 5	A 49	14	4E	3	8 2	1 75	12	6E	38	73 6	3	AFACTIO	N :	wa:sc					
00000000	0 65	72	76	69 6	3 6	3	57	1	1 1	4	50	43	6F	6F 6	E	Pruice:	5	NIPCont					
000080E	8 65	63	74	69 6	F 68	3	1 31	2	3 4	1 65	74	45	78	74 6	5	ection:	1 1	GetExte					
DOCOUDF	0 72	6E	61	6C 8	9 5	4	1 64	6	4 7:	2 65	73	73	CD	DA 5	s	rnalIPA	d t	iressU					
0086810	8 73	65	72	20 4	1 6	6	7. 6E	?	4 31	1 21	40	6F	78	69 6	C	ser-Age	9 1	: Mozil					
0008011	0 46	51	28	33 3	8 20		0 20	3	0 5	01	AF	10	11	20 2	8	NT 18 0	20	Ninéh.					
0008013	0 78	36	34	29 1	8 4	1 71	a 78	6	C 6	5.57	65	62	48	69 7	4	x64) Ap		eWebKit					
0000014	0 01	ac.	90	99 6	E 21	in.	1 28	. 9	0.14	1.44	Ch	hB	1.0	-	100	45.97.94		ACAD V DAY					

© 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.