

Every IT professional, from companies big or small, knows the value of data. Troubleshooting is always an act that is half instinct and half data – and Packet Sniffing is where the data comes in. **A Packet Sniffer is the tool that helps you figure out if packets are being sent, received, and arriving safely on your network,** but they can also do so much more!

Below is a list of some of the Network Analyzers and Sniffers and some of the features that they have built in for you **to extract network information and data.** They all tend to have the same sort of functionality – you can view packets being sent and received on some level or another, but many of the tools have certain nuances that allow them to shine in certain situations or network environments; the trick is knowing which one! Ultimately packet sniffing is the go to tool when you've got a network issue that you can't quite isolate to a single machine or protocol and it's time to start digging deep.

There's almost too many choices in this category of software. Some of them are a bit 'old-school'; they're grounded in terminal font and command-prompt interfaces and aren't that user friendly at first glance. Others are flashy much more geared towards a visual audience with easy installation, or portable executables, and plenty of graphs and tables. They also range from free to quite expensive for corporate licensing!

Ethereal

Ethereal is a freely available open source program that runs on almost any operating system. **Data from a network scan can be scanned in real time or scanned and saved for analyzing later.** For example, you could set up a script or schedule a scan to pinpoint something specific on your network, save it to a network drive, and analyze it at your convenience.

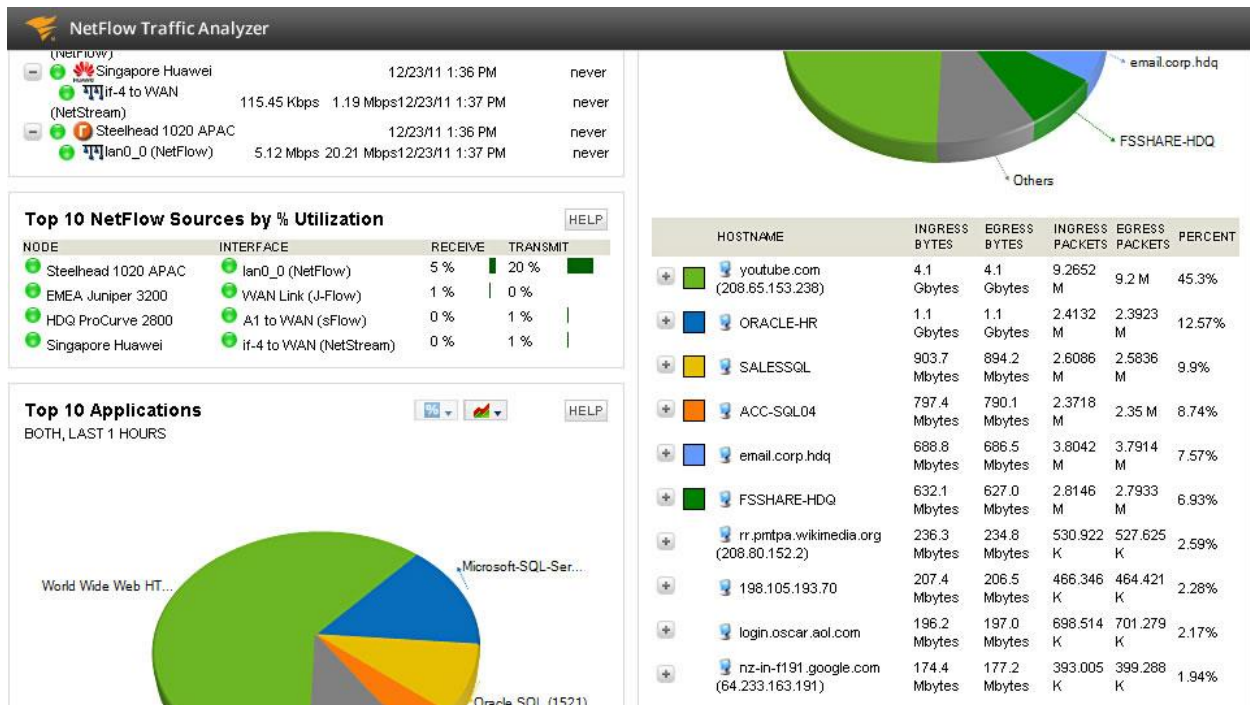
Ethereal is capable of dissecting 385 protocols including SMTP, ATM, IGRP, PPP, IPX and many more. **The program supports real-time scanning** of Ethernet, FDDI, Token Ring, IP over ATM, and even loopback interfaces on some machines. Ethereal also supports configurable filters to allow you to drill down on the particular data that you are interested in.

Solarwinds Bandwidth Analyzer 2-Pack



This particular software is a two-piece deal with similar, but distinct, functionality that goes hand in hand.

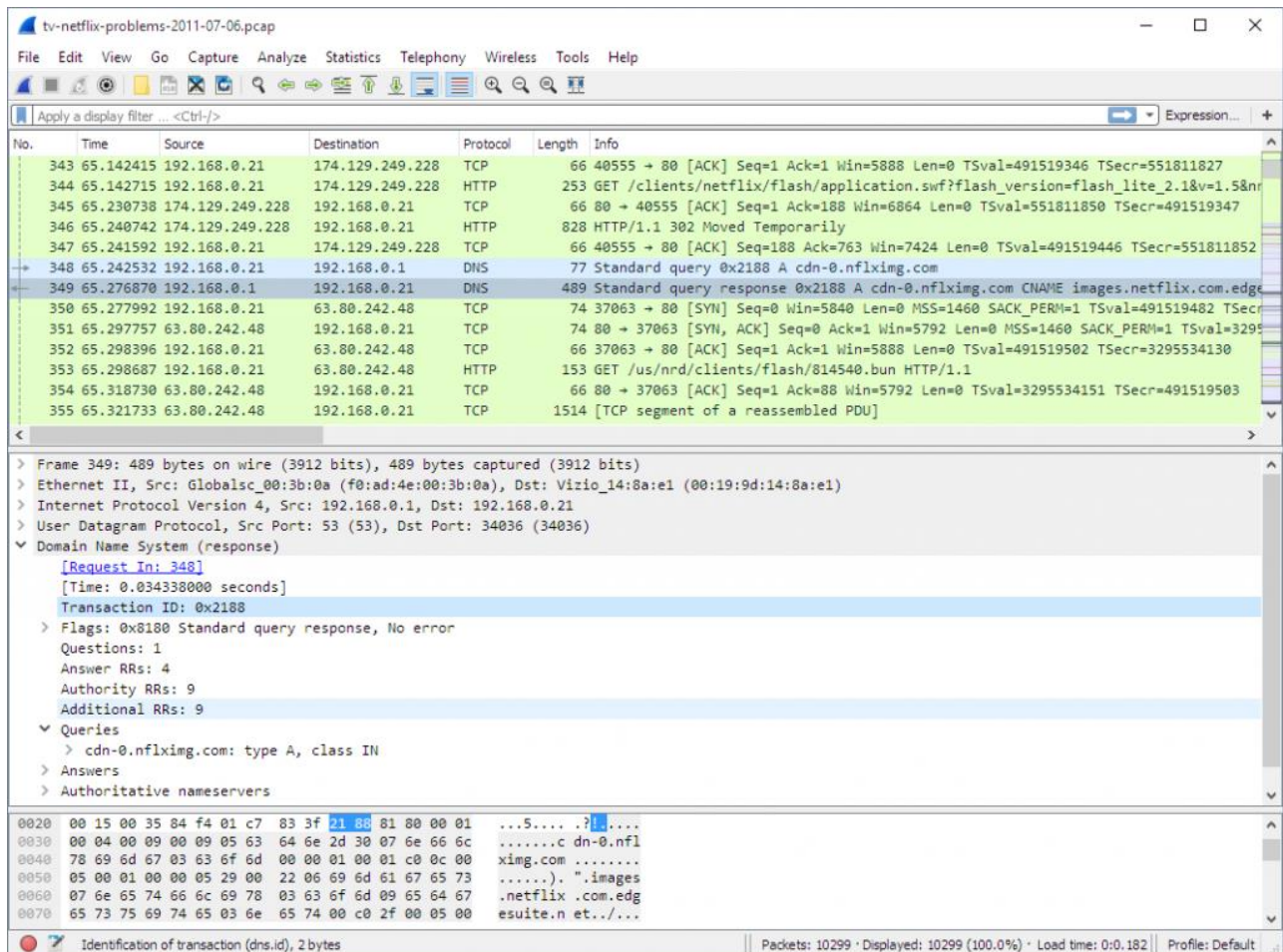
The Network Performance Monitor, as the name implies, monitors network performance and is going to be one of the Best Network Data Sniffers on the market if you want an **overall view of what's going on in your network**. What this means, more plainly, is it pays mind to more of the pure motility of the network. Transmission speeds and rates, packet transmission reliability, and even comes pre-configured with a wide variety of visual aids and sharp looking charts to make irregularities easier to spot.



Its counterpart, the Network Analyzer, again with a self-explanatory name, is more focused on the traffic itself. While the Performance Monitor is focused more on the overall view of the network's performance, the Network Analyzer is paying a lot more attention to the network on a more granular level.

In particular this part of the program ferrets out the bandwidth hogs and anomalies, sorted by merit of users, protocols, or applications. Available for Windows environments only.

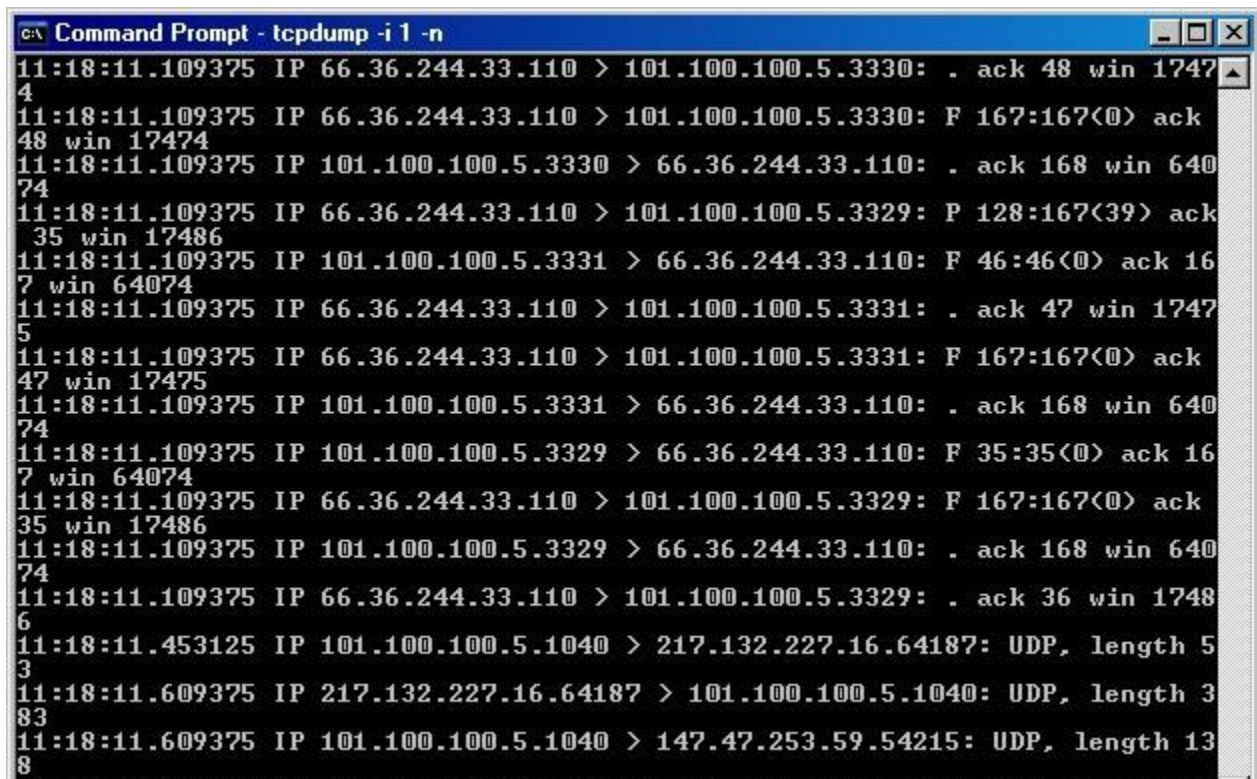
Wireshark



Wireshark is relatively new tool in the broad scheme of network diagnostics, and it does a great job finding a middle ground between raw data and visual representations of that data. It's simple, it's compatible, and it's portable. It does what needs doing and it does it succinctly.

It's got a clean UI, plenty of options for filtering and sorting, and, best of all for some of the multi-platform folks, it jives happily on any of the big three in terms of OS. Add to that the fact that it's open-source and a Free Sniffer and you've got a compelling tool to reach for when you need some quick diagnostics. Available for *NIX, Windows, and OSX environments.

Tcpdump

A screenshot of a Windows Command Prompt window titled "Command Prompt - tcpdump -i 1 -n". The window displays a series of network traffic capture lines from tcpdump. The output shows various IP addresses, ports, and flags (ack, P, F) along with sequence numbers and window sizes. The lines are formatted as timestamp:source_ip:source_port [IP destination_ip:destination_port] [flags] [sequence:window] [ack/seq]. The window has a standard Windows title bar with minimize, maximize, and close buttons.

```
C:\> Command Prompt - tcpdump -i 1 -n
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3330: . ack 48 win 1747
4
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3330: F 167:167<0> ack
48 win 17474
11:18:11.109375 IP 101.100.100.5.3330 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: P 128:167<39> ack
35 win 17486
11:18:11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: F 46:46<0> ack 16
7 win 64074
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: . ack 47 win 1747
5
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: F 167:167<0> ack
47 win 17475
11:18:11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: F 35:35<0> ack 16
7 win 64074
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: F 167:167<0> ack
35 win 17486
11:18:11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: . ack 36 win 1748
6
11:18:11.453125 IP 101.100.100.5.1040 > 217.132.227.16.64187: UDP, length 5
3
11:18:11.609375 IP 217.132.227.16.64187 > 101.100.100.5.1040: UDP, length 3
83
11:18:11.609375 IP 101.100.100.5.1040 > 147.47.253.59.54215: UDP, length 13
8
```

Tcpdump is something of an older tool and, to be frank, it looks like it. But there's a certain power in tools that are so cut and dry – it does what it needs to do, does it with as little a footprint as possible, and does it cleanly. It may be harder for some professionals to weed through the stark tables of data, but in some environments, or on a machine barely running, minimal is best.

It's native and has its origins in the *NIX environment, but there are several Windows ports that do the job well. It has all the functionality you'd want and need from a sniffer – capturing, recording, etc. – but it does lack a lot of the fancier capabilities of more robust software. Tcpdump is often called for due to its sheer reliability and simplicity. Available for *NIX and Windows environments.

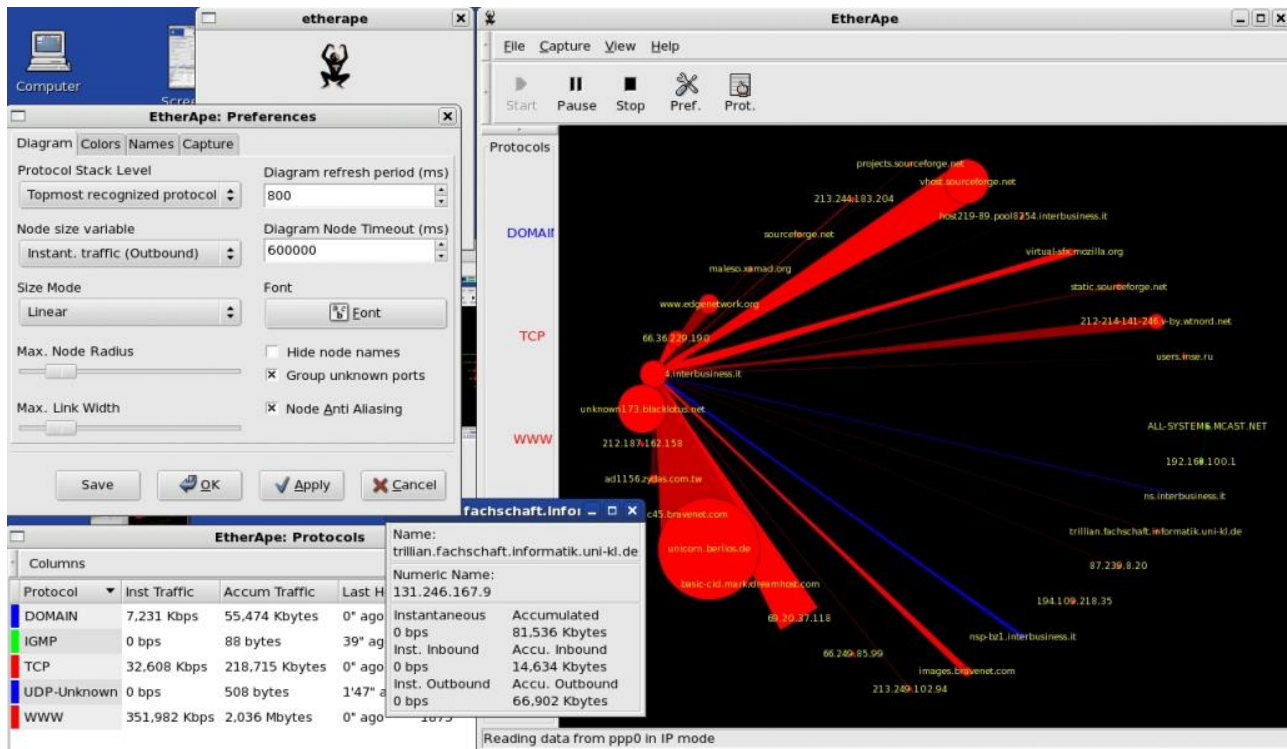
Kismet



Kismet is more than just a packet sniffer and, in fact, delves into wide range of functionality. Kismet even has the ability to sniff and analyze traffic of hidden networks or un-broadcasted SSIDs! Tools like this can be strangely invaluable in the right circumstances when there's something unknown causing troubles and you can't just find it – Kismet can sniff it out, if it happens to be a rogue network or AP acting up nobody mentioned they setup not quite right.

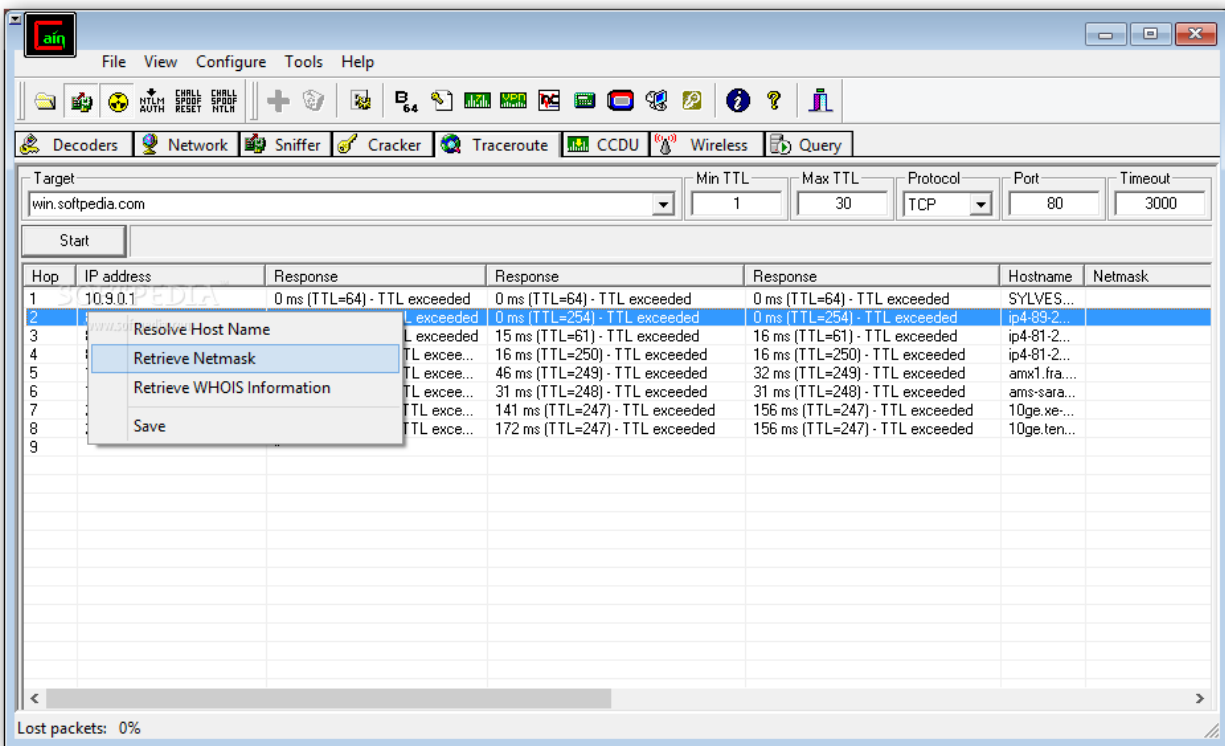
As one can imagine by the nature of wireless networking its a little more complex when it comes to sniffing, which is why a specialized tool like Kismet not only exists but is looked to frequently. Kismet is an excellent go to if you've got a lot of wireless traffic and wireless devices and need a tool that's better suited to handling a wireless-heavy network. Available for *NIX, Windows under Cygwin, and OSX environments.

EtherApe



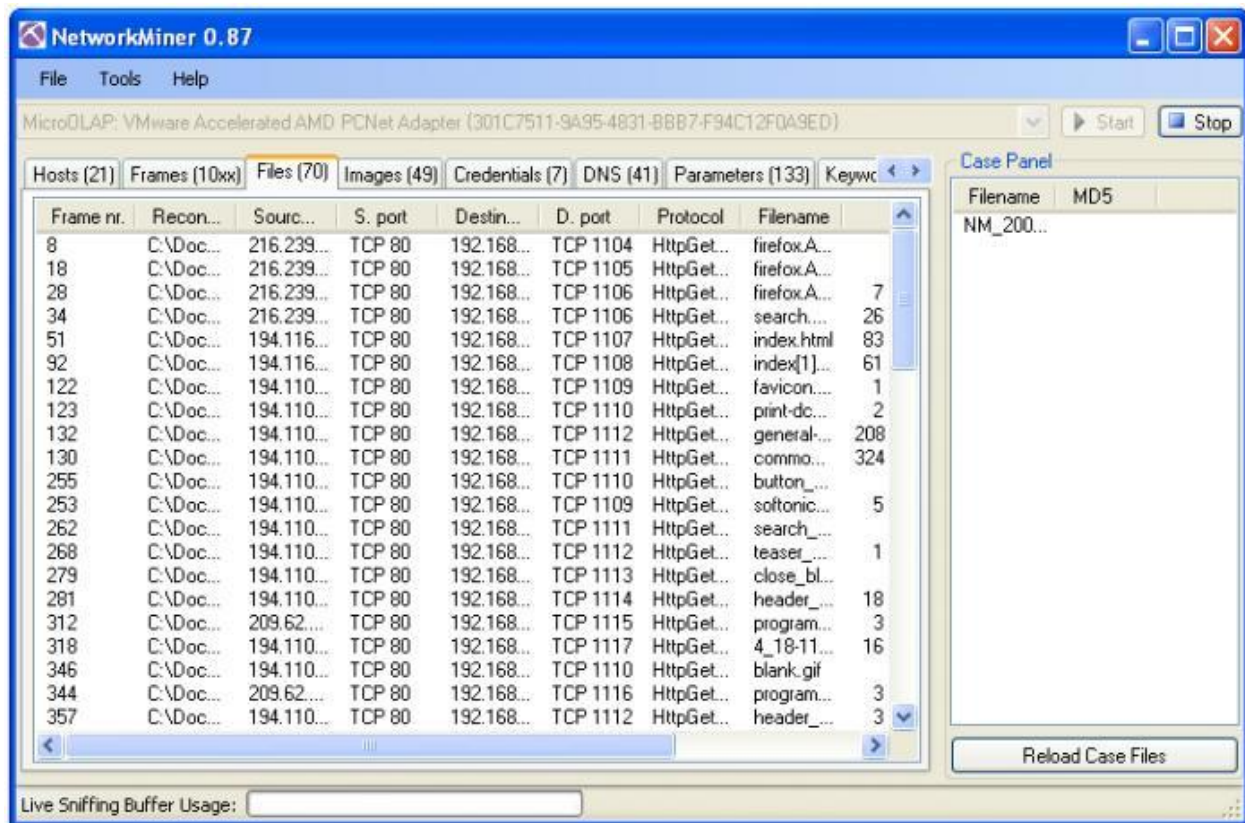
EtherApe has a lot of the same sort of functionality that WireShark does and, to boot, it also boasts being both Open-Source and free of any cost! What makes it different, though, is that it's far more graphically driven. Whereas WireShark has you peering at lists of numbers and comparing throughput in a more numerical sense, EtherApe takes the focus more to the visual and graphical realm. Some people just plain prefer the visual approach, and EtherApe tends to take precedence over WireShark for those folks. Available for *NIX and OSX environments.

Cain and Abel



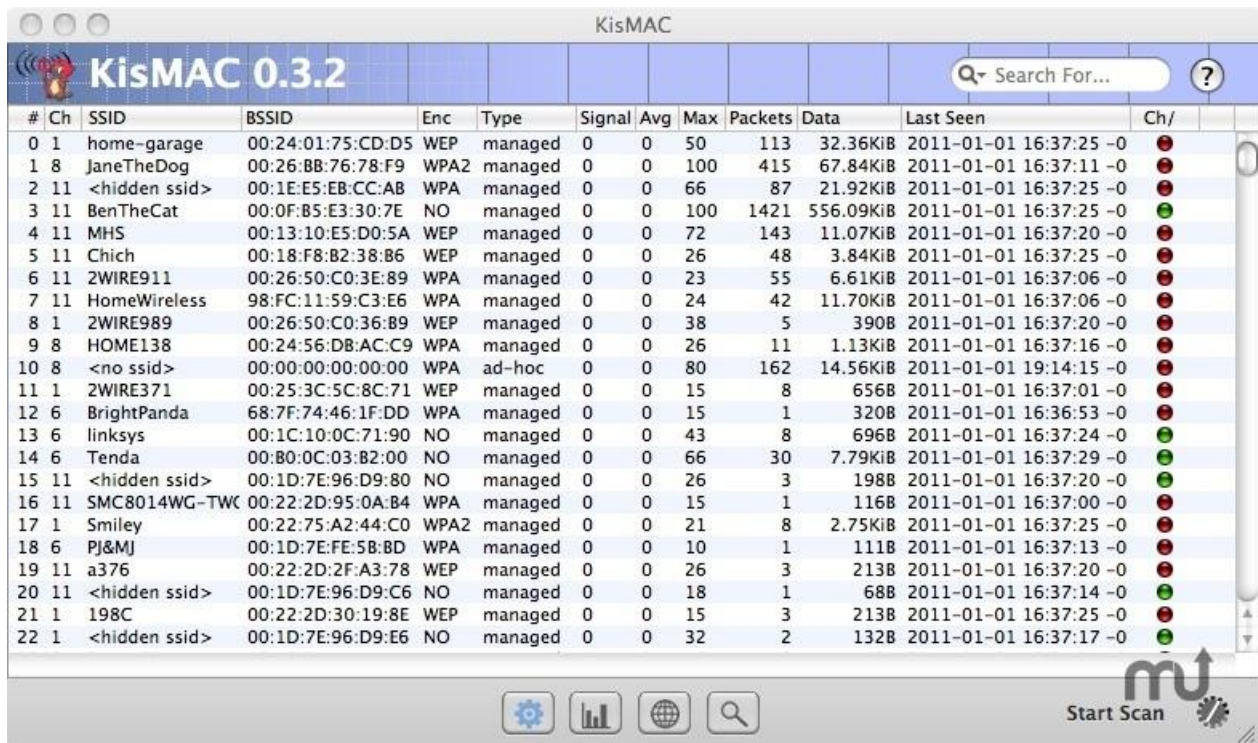
This particular software has a bit of a curious name, and it belies the remarkable breadth of tasks the program can perform. If your needs extend well beyond simple sniffing, then this may be the tool for you. It can even perform limited password recovery, do dictionary attacks to retrieve lost credentials, peruse VOIP data on the network, analyze routing, and so much more. This is a powerful tool that can really shine in those rare instances when you need to do a little search and recovery on a network. Available for Windows environments only.

NetworkMiner



Network miner is another tool that does more than sniff and, arguably, would be better suited to ferreting out problematic users or systems on a network than overall diagnosis or monitoring as a whole. Whereas other sniffers focus on the packets being sent back and forth, NetworkMiner is paying more mind to the ones doing the sending and receiving. An excellent tool for finding problem machines or users. Available for Windows environments only.

KisMAC



#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen	Ch/
0	1	home-garage	00:24:01:75:CD:D5	WEP	managed	0	0	50	113	32.36KiB	2011-01-01 16:37:25	-0
1	8	JaneTheDog	00:26:BB:76:78:F9	WPA2	managed	0	0	100	415	67.84KiB	2011-01-01 16:37:11	-0
2	11	<hidden ssid>	00:1E:E5:EB:CC:AB	WPA	managed	0	0	66	87	21.92KiB	2011-01-01 16:37:25	-0
3	11	BenTheCat	00:0F:B5:E3:30:7E	NO	managed	0	0	100	1421	556.09KiB	2011-01-01 16:37:25	-0
4	11	MHS	00:13:10:E5:D0:5A	WEP	managed	0	0	72	143	11.07KiB	2011-01-01 16:37:20	-0
5	11	Chich	00:18:F8:B2:38:B6	WEP	managed	0	0	26	48	3.84KiB	2011-01-01 16:37:25	-0
6	11	2WIRE911	00:26:50:C0:3E:89	WPA	managed	0	0	23	55	6.61KiB	2011-01-01 16:37:06	-0
7	11	HomeWireless	98:FC:11:59:C3:E6	WPA	managed	0	0	24	42	11.70KiB	2011-01-01 16:37:06	-0
8	1	2WIRE989	00:26:50:C0:36:89	WEP	managed	0	0	38	5	390B	2011-01-01 16:37:20	-0
9	8	HOME138	00:24:56:DB:AC:C9	WPA	managed	0	0	26	11	1.13KiB	2011-01-01 16:37:16	-0
10	8	<no ssid>	00:00:00:00:00:00	WPA	ad-hoc	0	0	80	162	14.56KiB	2011-01-01 19:14:15	-0
11	1	2WIRE371	00:25:3C:5C:8C:71	WEP	managed	0	0	15	8	656B	2011-01-01 16:37:01	-0
12	6	BrightPanda	68:7F:74:46:1F:DD	WPA	managed	0	0	15	1	320B	2011-01-01 16:36:53	-0
13	6	linksys	00:1C:10:0C:71:90	NO	managed	0	0	43	8	696B	2011-01-01 16:37:24	-0
14	6	Tenda	00:80:0C:03:B2:00	NO	managed	0	0	66	30	7.79KiB	2011-01-01 16:37:29	-0
15	11	<hidden ssid>	00:1D:7E:96:D9:80	NO	managed	0	0	26	3	198B	2011-01-01 16:37:20	-0
16	11	SMC8014WG-TW	00:22:2D:95:0A:B4	WPA	managed	0	0	15	1	116B	2011-01-01 16:37:00	-0
17	1	Smiley	00:22:75:A2:44:C0	WPA2	managed	0	0	21	8	2.75KiB	2011-01-01 16:37:25	-0
18	6	PJ&MJ	00:1D:7E:FE:5B:BD	WPA	managed	0	0	10	1	111B	2011-01-01 16:37:13	-0
19	11	a376	00:22:2D:2F:A3:78	WEP	managed	0	0	26	3	213B	2011-01-01 16:37:20	-0
20	11	<hidden ssid>	00:1D:7E:96:D9:C6	NO	managed	0	0	18	1	68B	2011-01-01 16:37:14	-0
21	1	198C	00:22:2D:30:19:8E	WEP	managed	0	0	15	3	213B	2011-01-01 16:37:25	-0
22	1	<hidden ssid>	00:1D:7E:96:D9:E6	NO	managed	0	0	32	2	132B	2011-01-01 16:37:17	-0

This software's name says it all – it's a lot like Kismet, but for the Mac environment. KisMAC! Simple as that. These days Kismet has a Mac environment port, so it may seem redundant, but it's worth emphasizing that KisMAC actually has its own codebase and was not directly derivative from Kismet's. Of particular note is that it offers several mapping and de-auth features on Mac that Kismet itself doesn't provide, and due to its unique codebase you may find it does the job better than Kismet itself at times. Available for OSX environments only.