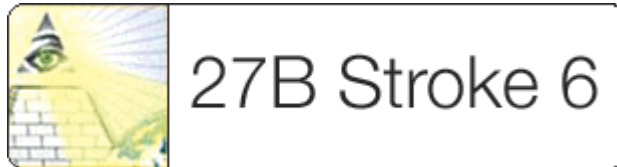




Does your managed hosting provider cost your business
More than you thought it would?



by [Ryan Singel](#) and [Kevin Poulsen](#)

Tuesday, 27 June 2006

The Newbie's Guide to Detecting the NSA



It's not surprising that an expert hired by EFF should produce an analysis that supports the group's case against AT&T. But last week's public court filing of a redacted statement by J. Scott Marcus is still worth reading for the obvious expertise of its author, and the cunning insights he draws from the AT&T spy documents.

An internet pioneer and former FCC advisor who held a Top Secret security clearance, Marcus applies a Sherlock Holmes level of reasoning to his dissection of the evidence in the case: 120-pages of AT&T manuals that EFF filed under seal, and whistleblower Mark Klein's observations inside the company's San Francisco switching center.

If you've been following Wired News' [coverage](#) of the EFF case, you won't find many new hard revelations in [Marcus' analysis](#) -- at least, not in the censored version made public. But he connects the dots to draw some interesting conclusions:

- **The AT&T documents are authentic.** That AT&T insists they remain under seal is evidence enough of this, but Marcus points out that the writing style is pure Bell System, with the "meticulous attention to detail that is typical of AT&T operations."
- **There may be dozens of surveillance rooms in AT&T offices around the country.** Among other things, Marcus finds that portions of the documents are written to cover a number of different equipment rack configurations, "consistent with a deployment to 15 to 20" secret rooms.
- **The internet surveillance program covers domestic traffic, not just international traffic.** Marcus notes that the AT&T spy rooms are "in far more locations than would be required to catch the majority of international traffic"; the configuration in the San Francisco office promiscuously sends all data into the secret room; and there's no reliable way an analysis could infer a user's physical location from their IP address. This, of course, directly contradicts President Bush's description of the "Terrorist Surveillance Program."
- **The system is capable of looking at content, not just addresses.** The configuration described in the Klein documents -- presumably the [Narus software](#) in particular -- "exists primarily to conduct sophisticated rule-based analysis of content", Marcus concludes.

My bullet points don't come close to conveying the painstaking reasoning he lays out to back each of his conclusions.

Perhaps the most interesting -- and, in retrospect, obvious -- point Marcus makes is that AT&T customers aren't the only ones apparently being tapped. "Transit" traffic originating with one ISP and destined for another is also being sniffed if it crosses AT&T's network. Ironically, because the taps are installed at the point at which that network connects to the rest of the world, the safest web surfers are AT&T subscribers visiting websites hosted on AT&T's network. Their traffic doesn't pass through the splitters.

With that in mind, here's the *27B Stroke 6* guide to detecting if your traffic is being funneled into the secret room on San Francisco's Folsom street.

If you're a Windows user, fire up an MS-DOS command prompt. Now type **tracert** followed by the domain name of the website, e-mail host, VoIP switch, or whatever destination you're interested in. Watch as the program spits out your route, line by line.

```
C:\> tracert nsa.gov

 1  2 ms  2 ms  2 ms  12.110.110.204
    [...]
 7 11 ms 14 ms 10 ms as-0-0.bbr2.SanJose1.Level3.net [64.159.0.218]
 8 13 12 19 ms ae-23-56.car3.SanJose1.Level3.net [4.68.123.173]
 9 18 ms 16 ms 16 ms 192.205.33.17
10 88 ms 92 ms 91 ms tbr2-p012201.sffca.ip.att.net [12.123.13.186]
11 88 ms 90 ms 88 ms tbr1-cl2.sl9mo.ip.att.net [12.122.10.41]
12 89 ms 97 ms 89 ms tbr1-cl4.wswdc.ip.att.net [12.122.10.29]
13 89 ms 88 ms 88 ms ar2-a3120s6.wswdc.ip.att.net [12.123.8.65]
14 102 ms 93 ms 112 ms 12.127.209.214
15 94 ms 94 ms 93 ms 12.110.110.13
16 * * *
17 * * *
18 * *
```

In the above example, my traffic is jumping from Level 3 Communications to AT&T's network in San Francisco, presumably over the OC-48 circuit that AT&T **tapped** on February 20th, 2003, according to the Klein docs.

The magic string you're looking for is **sffca.ip.att.net**. If it's present immediately above or below a non-**att.net** entry, then -- by Klein's allegations -- your packets are being copied into room 641A, and from there, illegally, to the NSA.

Of course, if Marcus is correct and AT&T has installed these secret rooms all around the country, then any **att.net** entry in your route is a bad sign.

Posted by Kevin Poulsen at 11:18 AM PDT | [Post Comment](#) | [View Comments \(37\)](#) | [Permalink](#)

Thursday, 29 June 2006 - 9:36 AM PDT

Name: "TC"

I had to give it a try... linux traceroute gives much more detailed information. Notice how in lines 10-12 I appear to go from NY to DC back to NY...

```
$ traceroute english.aljazeera.net
traceroute to 199.106.212.27 (199.106.212.27), 30 hops max, 38 byte packets
 1  10.250.1.1 (10.250.1.1)
 2  10.23.1.1 (10.23.1.1)
 3  at-1-0-0-1711.CORE-RTR2.HAG.verizon-gni.net (130.81.12.17)
 4  so-1-3-0-0.CORE-RTR1.HAG.verizon-gni.net (130.81.18.244)
    MPLS Label=112000 CoS=2 TTL=1 S=1
 5  so-3-3-1-0.BB-RTR1.RES.verizon-gni.net (130.81.20.20)
    MPLS Label=114896 CoS=2 TTL=1 S=1
 6  so-6-0-0-0.ASH-PEER-RTR2.verizon-gni.net (130.81.17.177)
 7  0.so-7-0-0.XL2.IAD8.ALTER.NET (152.63.36.205)
 8  0.so-0-1-0.XL2.DCA5.ALTER.NET (152.63.32.33)
 9  0.so-7-0-0.BR1.DCA5.ALTER.NET (152.63.43.177)
10  telia-gw.n54ny.ip.att.net (192.205.32.49)
11  tbr2-p011901.wswdc.ip.att.net (12.123.8.110)
    MPLS Label=32752 CoS=0 TTL=1 S=1
12  tbr2-cl15.n54ny.ip.att.net (12.122.10.53)
    MPLS Label=31468 CoS=0 TTL=1 S=1
13  gar5-p390.n54ny.ip.att.net (12.123.3.13)
14  mdf16-gsr12-1-pos-6-0.nyc2.attens.com (12.122.255.114)
```

15 mdf20-bi4k-2-eth-2-1.attens.net (63.240.18.6)

16 *

[Reply to this Comment](#)

Thursday, 29 June 2006 - 9:45 AM PDT

Name: Bill

Just because the hostname appears to have a geographical name, doesn't mean that the router resides in that area. A traceroute tells you nothing of the gateway's physical location. Who's to say that that host isn't a gateway to AT&T's DC facility, but housed in the NY facility, and your traffic is routing through it to get to host #12, because there's a cable cut between host 10 and 12?

Quick! Scramble the black helicopters!

[Reply to this Comment](#)

Thursday, 29 June 2006 - 9:57 AM PDT

Name: "hal"

if there is a router capturing traffic, and if it has a fast route to the organisation capturing traffic, and if it is advertising it (it probably shouldn't but such things are easy to misconfigure), then it is entirely normal that it shows up in a traceroute to that organisation. you should be worried if such routers show up in other traceroutes. on the other hand, it is trivial to not have a sniffing router show up. ever wondered why sometimes your packets pass entire backbones and all you see are the entry and exit points? easy. they encapsulate your packets in a different protocol, and as far as ip is concerned, there are no hops in between. heck, any old ethernet bridge built from a \$50 junkyard pc can do that (sniff your traffic without showing up in traceroute) and you have no possibility of detecting it unless you are on one of the directly connected network segments.

[Reply to this Comment](#)

Thursday, 29 June 2006 - 10:27 AM PDT

Name: Tom

If that is the case why do they put city names in the host name.

tbr2012701.phmaz.ip.att.net [12.123.206.30]

tbr2-cl1592.dlstx.ip.att.net [12.122.10.81]

tbr1-cl6.sl9mo.ip.att.net [12.122.10.89]

tbr1-cl4.wswdc.ip.att.net [12.122.10.29]

ar2-a3120s6.wswdc.ip.att.net [12.123.8.65]

[Reply to this Comment](#)

Thursday, 29 June 2006 - 11:04 AM PDT

Name: WUXIA

City From IP

<http://www.dnsstuff.com/>

tbr2012701.phmaz.ip.att.net [12.123.206.30]

City: Morristown, New Jersey

tbr2-cl1592.dlstx.ip.att.net [12.122.10.81]

City: Morristown, New Jersey

tbr1-cl6.sl9mo.ip.att.net [12.122.10.89]

City: Fargo, North Dakota

tbr1-cl4.wswdc.ip.att.net [12.122.10.29]

City: Fargo, North Dakota

ar2-a3120s6.wswdc.ip.att.net [12.123.8.65]

Thursday, 29 June 2006 - 11:24 AM PDT

Name: "xox"

Home Page: <http://thehun.net>

There are a number of different commercial products to sniff data directly off of the fiber without a hop even appearing. It doesn't matter who the provider is, the feds are setup with all the major players to allow them to sniff their traffic and pull all the info they need. Generally br is border router and ar is access router so is sonet link. The router and interface IPs don't really have to map to the exact city/state because they are probably registered through a locality and then broken into pieces. They're not trying to trick you by misleading the dns naming, it really is easy to sniff that traffic, how to sort and manage all that data coming off the pipe is another story altogether.

[Reply to this Comment](#)

Thursday, 29 June 2006 - 11:37 AM PDT

Name: "anonymous"

12 253 ms 291 ms 284 ms tbr1010901.attga.ip.att.net [12.122.81.98]

[Reply to this Comment](#)

Thursday, 29 June 2006 - 11:46 AM PDT

Name: "s"

Please correct me if I'm wrong. Assuming no other ISPs/core-network owners are doing the same thing for the NSA - you should only really be worried if you are accessing network services that you need to hop through an AT&T-owned network to access, correct? Sure, tracerouting nsa.gov or att.com will traverse AT&T's network and you will see that tbr1-... host, located wherever. But a few random traceroutes to other hosts - google, slashdot, nytimes, mspace - and I don't see those sketchy AT&T hosts. So is the bottom-line to avoid traversing AT&T's networks? I've got my fingers crossed Sprint isn't doing the same thing.

[Reply to this Comment](#)

Thursday, 29 June 2006 - 11:56 AM PDT

Name: "bahiabob"

Home Page: <http://bahiabob@pipeline.com>

So now you are emulating the proterrorist antiAmerican NYT??? Thanks for tipping the hand to all terrorists on the net. How stupid can you lefties get? Thanks again for your treasonist diatribe on how to defeat the NSA and the USA. When the Zarquai's come for you, I hope you enjoy your beheading. Don't forget to kiss your azz goodbye. Now would be a good time.

[Reply to this Comment](#)

Thursday, 29 June 2006 - 12:12 PM PDT

Name: s

gotta love the internet!

"Militant Libertarian Cowboy and defender of truth, justice and the American Way. I don't care for "media spin" and I will not ever spin anything. Only the real truth and tellers of the same need apply. I write this blog for ME not you. If you want feelings and touchy-feely get a therapist and quit bothering me. If you are a whining, liberal Democrat or someone who thinks Mickey Mouse Moore tells the truth, see above. If you live in the lefty city by the bay or La La Land and voted for Boxer, Pelosi, Feinstein or Waxman, get a life, a brain, a haircut and a REAL job."

Last time I checked, we have laws, when laws are broken, people should be held accountable.

[Reply to this Comment](#)

[View Latest Entries](#)

June 2006						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Entries by Topic

[All topics](#) <

Group One

- [Tripod Home](#)
- [Tripod Build](#)
- [Tripod Member](#)
- [Spotlight](#)
- [Webmonkey Tools](#)
- [Register Your Domain](#)

Group Two

- [Lycos Home](#)
- [Blog Anywhere](#)
- [Blog Reader](#)
- [Lycos Search](#)
- [Wired News](#)

[XML](#)

You are not logged in.

[Log in](#)



Wired News: [Contact Us](#) | [Advertising](#) | [Subscribe](#)

We are translated daily into Korean and Japanese

© Copyright 2006, Lycos, Inc. Lycos is a registered trademark of Lycos, Inc. All Rights Reserved.

Your use of this website constitutes acceptance of the Lycos **Privacy Policy** and **Terms & Conditions**