#BruCON

The Curious Case of 42.0.20.80

WE NEED HELP!

The Curious Case of 42.0.20.80

@MRKOOT

@YAFSEC

The Curious Case of 42.0.20.80

$ host -t a www.google.com

www.google.com has address 42.0.20.80

The Curious Case of 42.0.20.80

netnum: 42.0.16.0 - 42.0.23.255
netname: CHINANET-GD
descr: CHINANET Guangdong province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: IC83-AP
status: ALLOCATED PORTABLE
notify: [...redacted...]
remarks: service provider
changed: [...redacted...] 20110412
mnt-by: APNIC-HM
mnt-lower: MAINT-CHINANET-GD
mnt-irt: IRT-CHINANET-CN
source: APNIC

The Curious Case of 42.0.20.80

@mrkoot

What's up with @Google domains incidentally resolving to 42.0.20.80, owned by China Telecom (Guangdong)? Is that bonafide?

@Yafsec:

@mrkoot If the resolver uses gethostbyname, it expects ipv4. When on ipv6 it apparently uses the first 4 bytes of the ipv6 address as ipv4.

The Curious Case of 42.0.20.80

$ host -t aaaa www.google.com

www.google.com has IPv6 address 2a00:1450:4013:c00::63

....but I only now noticed that the first four bytes of that address, 2a00:1450, hexadecimally represent 42.0.20.80!

The Curious Case of 42.0.20.80

UPDATE 2013-03-10: everything is caused by this bug in dproxy, a caching DNS proxy that runs on the Conceptronic C54APRB2+ router. Tip of the hat to the anonymous commenter who suggested this!

The Curious Case of 42.0.20.80

$ host -t a ipv6.l.google.com

ipv6.l.google.com has no A record

$ host -t aaaa ipv6.l.google.com

ipv6.l.google.com has IPv6 address 2a00:1450:400c:c05::68

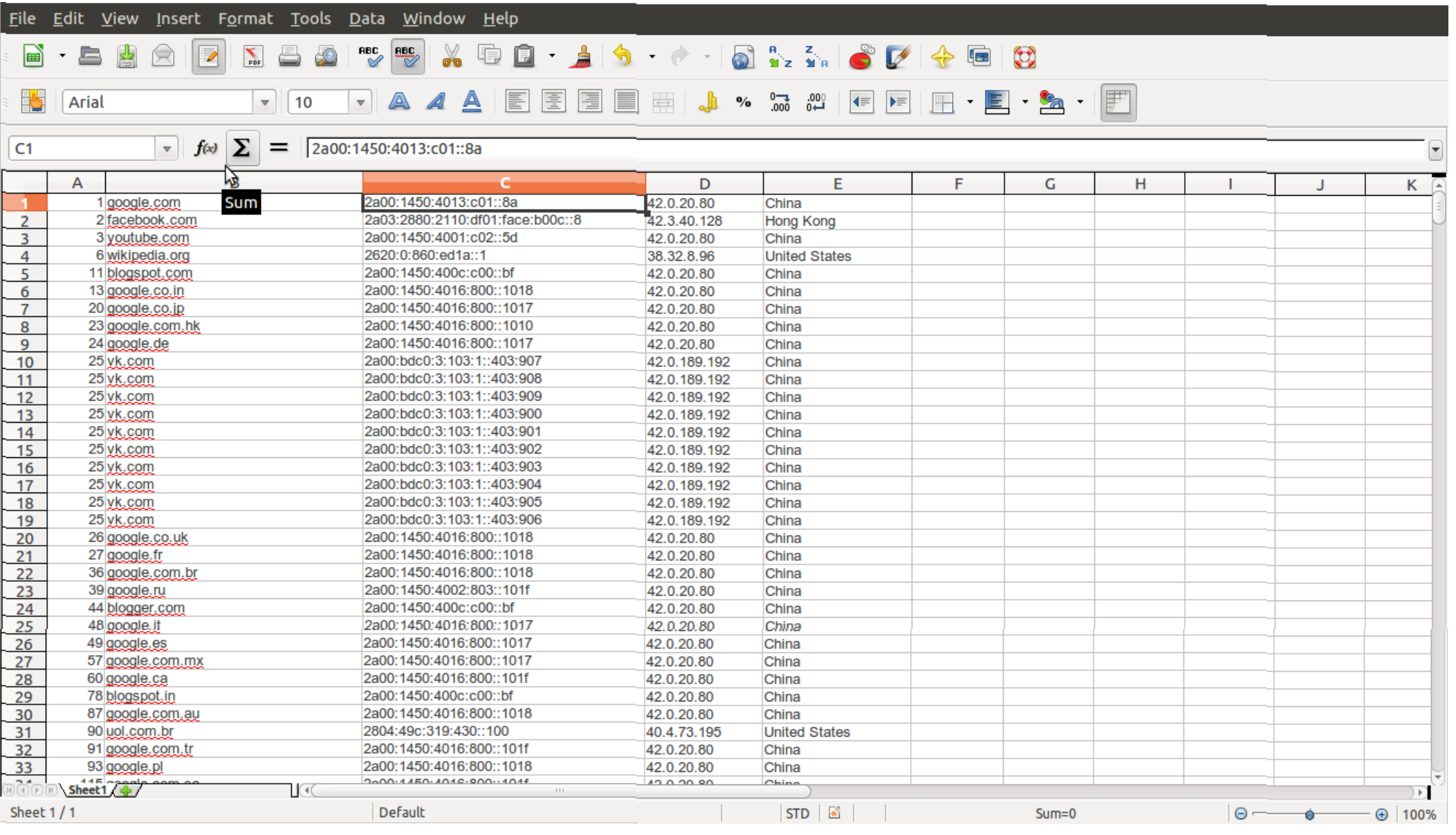
$ host -t a ipv6.l.google.com

ipv6.l.google.com has address 42.0.20.80

The Curious Case of 42.0.20.80

```
try:
        answers = dns.resolver.query(qu, 'AAAA')
        for rdata in answers:
            print 'IPv6 address : ' + rdata.address
            a = rdata.address.replace(':',"")[:8]
            i = 0
            addr = ''
            while i < 8:
                j=i+2
                addr = addr + str((int(a[i:j],16)))
                if i < 6:
                    addr = addr + '.'
                i=j
            print 'IPv4 target  : ' + addr
    except:
        print 'No IPv6 record found'
        return
```

The Curious Case of 42.0.20.80



File Edit View Insert Format Tools Data Window Help

Arial 10

C1 | Σ | = | 2a00:1450:4013:c01::8a

Sum

	A		C	D	E	F	G	H	I	J	K
1	1	google.com	2a00:1450:4013:c01::8a	42.0.20.80	China						
2	2	facebook.com	2a03:2880:2110:df01:face:b00c::8	42.3.40.128	Hong Kong						
3	3	youtube.com	2a00:1450:4001:c02::5d	42.0.20.80	China						
4	6	wikipedia.org	2620:0:860:ed1a::1	38.32.8.96	United States						
5	11	blogspot.com	2a00:1450:400c:c00::bf	42.0.20.80	China						
6	13	google.co.in	2a00:1450:4016:800::1018	42.0.20.80	China						
7	20	google.co.jp	2a00:1450:4016:800::1017	42.0.20.80	China						
8	23	google.com.hk	2a00:1450:4016:800::1010	42.0.20.80	China						
9	24	google.de	2a00:1450:4016:800::1017	42.0.20.80	China						
10	25	vk.com	2a00:bdc0:3:103:1::403:907	42.0.189.192	China						
11	25	vk.com	2a00:bdc0:3:103:1::403:908	42.0.189.192	China						
12	25	vk.com	2a00:bdc0:3:103:1::403:909	42.0.189.192	China						
13	25	vk.com	2a00:bdc0:3:103:1::403:900	42.0.189.192	China						
14	25	vk.com	2a00:bdc0:3:103:1::403:901	42.0.189.192	China						
15	25	vk.com	2a00:bdc0:3:103:1::403:902	42.0.189.192	China						
16	25	vk.com	2a00:bdc0:3:103:1::403:903	42.0.189.192	China						
17	25	vk.com	2a00:bdc0:3:103:1::403:904	42.0.189.192	China						
18	25	vk.com	2a00:bdc0:3:103:1::403:905	42.0.189.192	China						
19	25	vk.com	2a00:bdc0:3:103:1::403:906	42.0.189.192	China						
20	26	google.co.uk	2a00:1450:4016:800::1018	42.0.20.80	China						
21	27	google.fr	2a00:1450:4016:800::1018	42.0.20.80	China						
22	36	google.com.br	2a00:1450:4016:800::1018	42.0.20.80	China						
23	39	google.ru	2a00:1450:4002:803::101f	42.0.20.80	China						
24	44	blogger.com	2a00:1450:400c:c00::bf	42.0.20.80	China						
25	48	google.it	2a00:1450:4016:800::1017	42.0.20.80	China						
26	49	google.es	2a00:1450:4016:800::1017	42.0.20.80	China						
27	57	google.com.mx	2a00:1450:4016:800::1017	42.0.20.80	China						
28	60	google.ca	2a00:1450:4016:800::101f	42.0.20.80	China						
29	78	blogspot.in	2a00:1450:400c:c00::bf	42.0.20.80	China						
30	87	google.com.au	2a00:1450:4016:800::1018	42.0.20.80	China						
31	90	uol.com.br	2804:49c:319:430::100	40.4.73.195	United States						
32	91	google.com.tr	2a00:1450:4016:800::101f	42.0.20.80	China						
33	93	google.pl	2a00:1450:4016:800::1018	42.0.20.80	China						

Sheet1

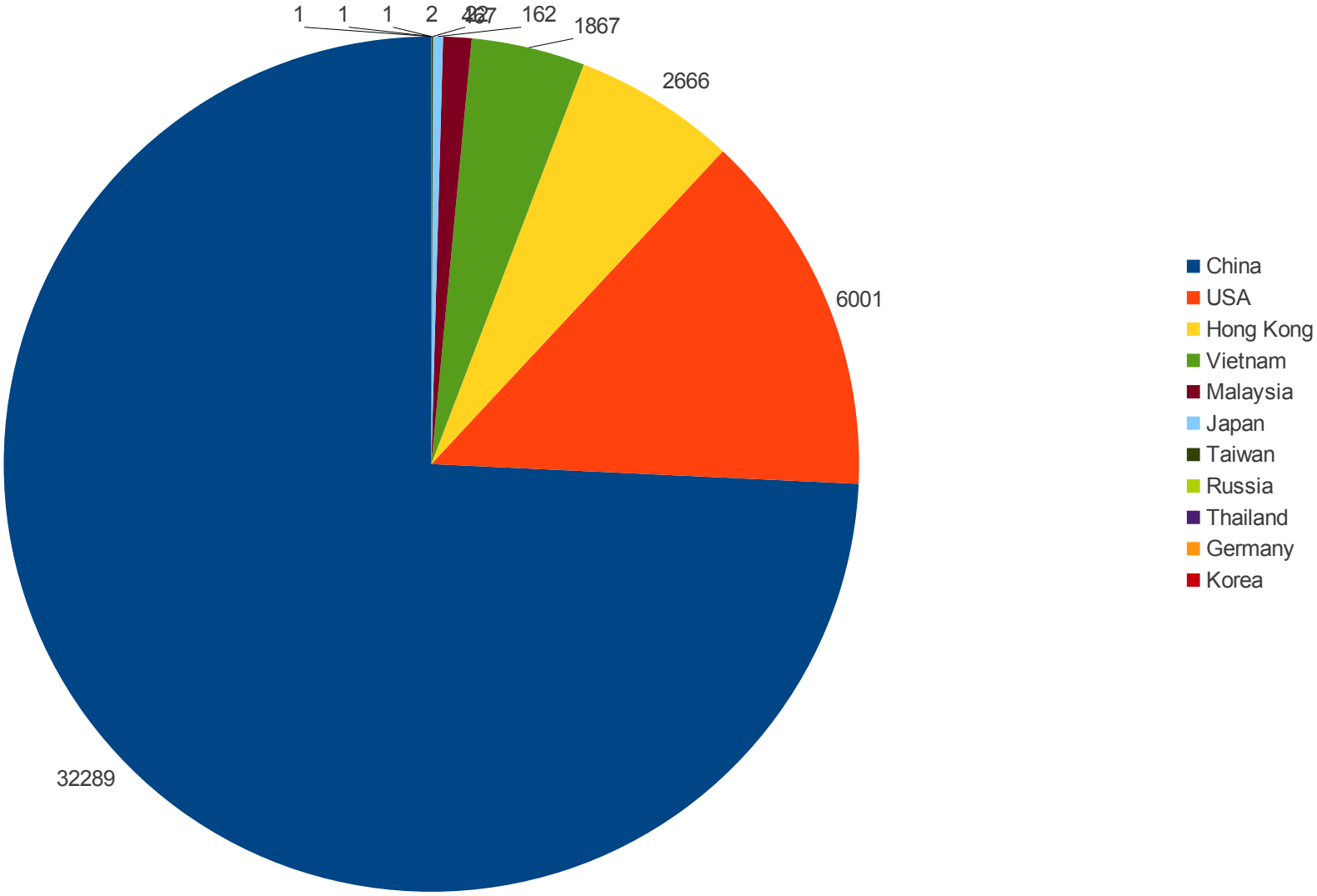
Sheet 1 / 1 | Default | STD | Sum=0 | 100%

The Curious Case of 42.0.20.80

So, we did it on the Alexa top1000000 domains....

Only 43500 have IPV6....

The Curious Case of 42.0.20.80



The Curious Case of 42.0.20.80

Data Table

Column 1

	Categories	Y-Values
1	China	32289
2	USA	6001
3	Hong Kong	2666
4	Vietnam	1867
5	Malaysia	467
6	Japan	162
7	Taiwan	22
8	Russia	2
9	Thailand	1
10	Germany	1
11	Korea	1

The Curious Case of 42.0.20.80

So, do you know people that own IP's?

We need your help!!!

@YAFSEC

http://pastebin.com/4zabmBHU