#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

```python
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
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

<table>
<thead>
<tr>
<th>Categories</th>
<th>Y-Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>32289</td>
</tr>
<tr>
<td>USA</td>
<td>6001</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>2666</td>
</tr>
<tr>
<td>Vietnam</td>
<td>1867</td>
</tr>
<tr>
<td>Malaysia</td>
<td>467</td>
</tr>
<tr>
<td>Japan</td>
<td>162</td>
</tr>
<tr>
<td>Taiwan</td>
<td>22</td>
</tr>
<tr>
<td>Russia</td>
<td>2</td>
</tr>
<tr>
<td>Thailand</td>
<td>1</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
</tr>
<tr>
<td>Korea</td>
<td>1</td>
</tr>
</tbody>
</table>
The Curious Case of 42.0.20.80

So, do you know people that own IP's?
We need your help!!!