DNS Privacy

QNAME Minimization and IETF DPRIVE WG

Warren Kumari

What's the problem?

I hate doing expense reports…

so I procrastinate…

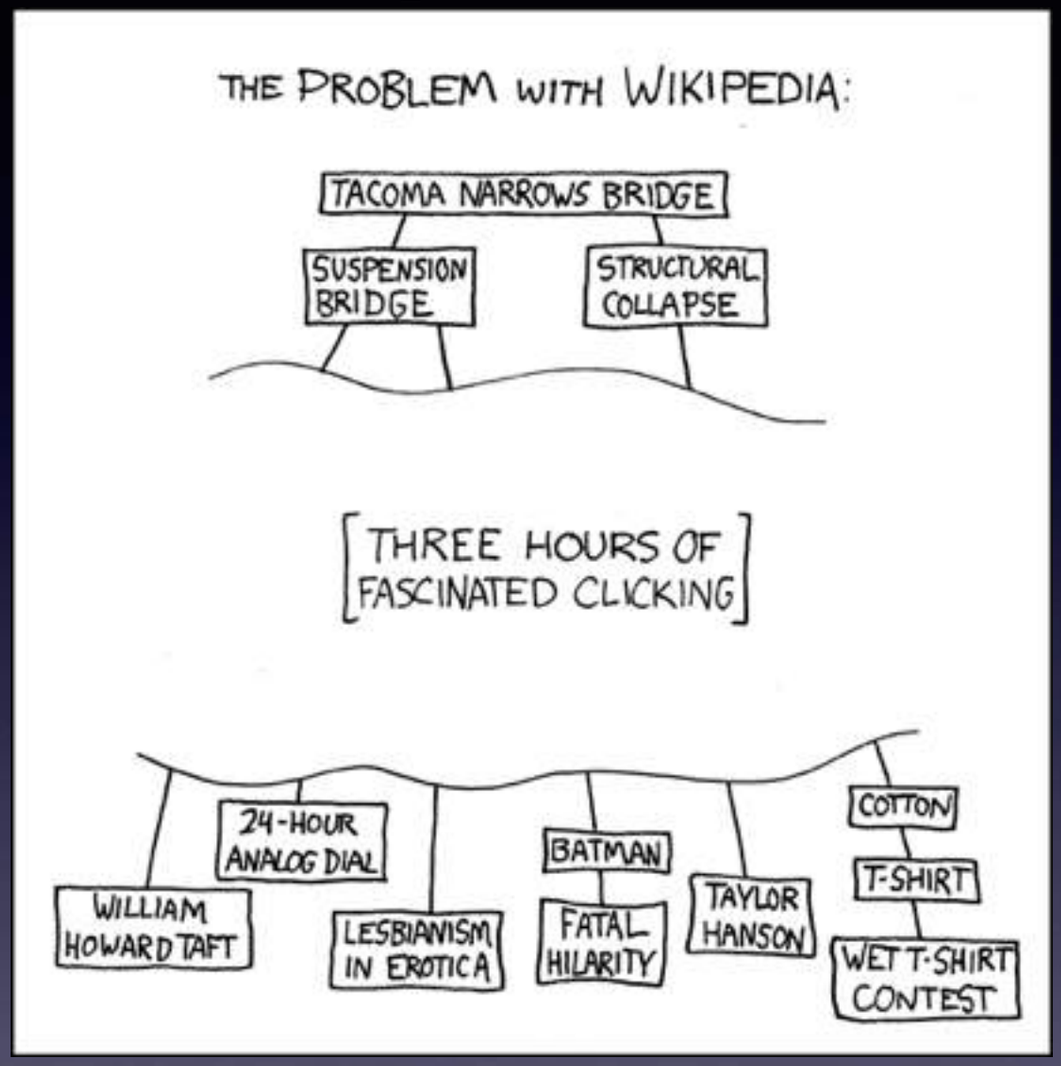
… and tidy up my desk

… and clean all the crumbs out of my keyboard

… and do the laundry

… and then start reading Wikipedia….

What's the problem? (cont)



"99 Luftballons"→ "99 Red Balloons"→ Nuclear accidents → [Three hours of fascinated clicking] → websites on the efficiency of centrifugal enrichment of uranium-235

So what?

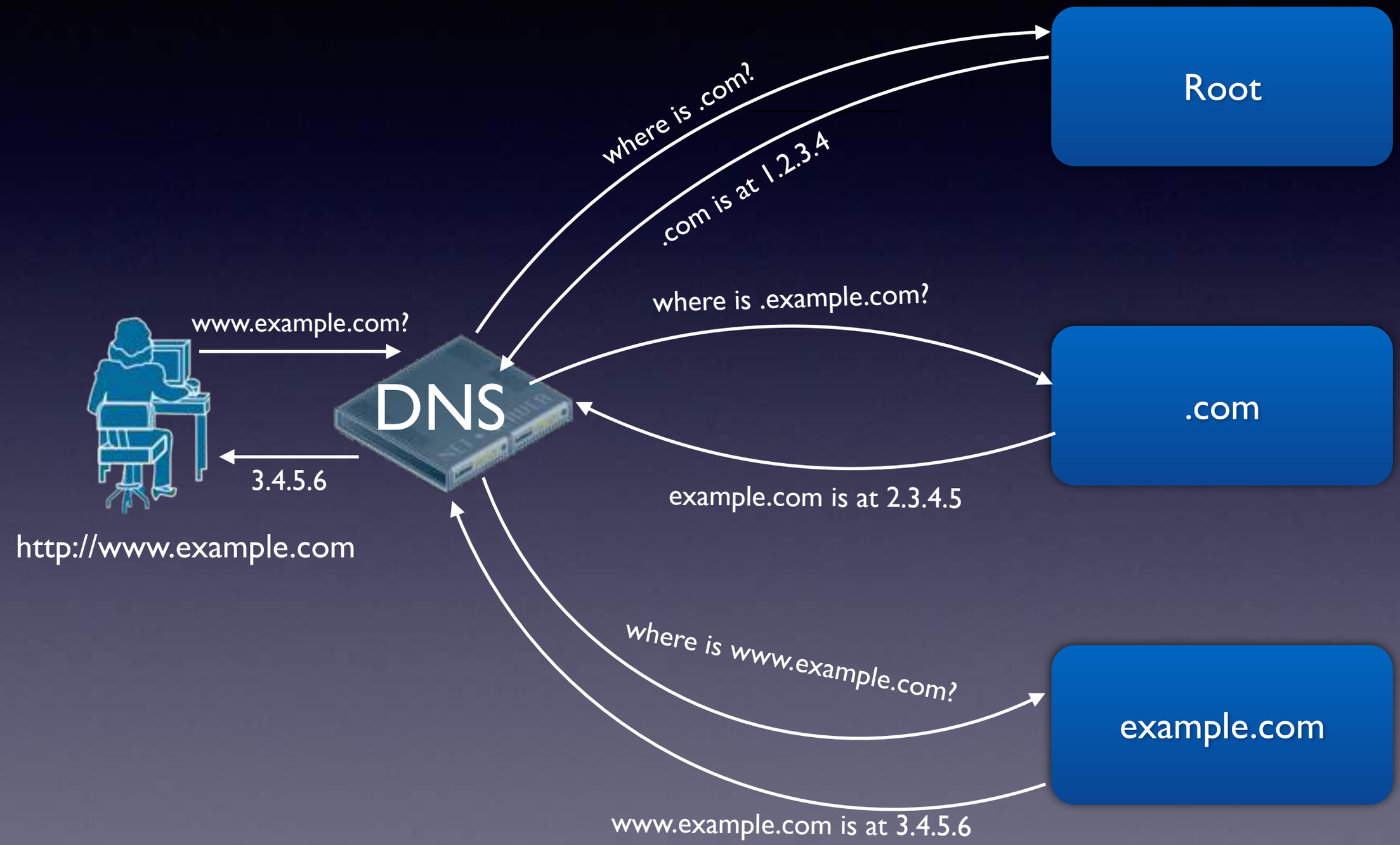
All of the URLs I went to were https:// , so the content is protected, no-one is likely to get the wrong idea…

…but many of the domain names that my machine looked up were, um, suspicious, especially if taken out of context.

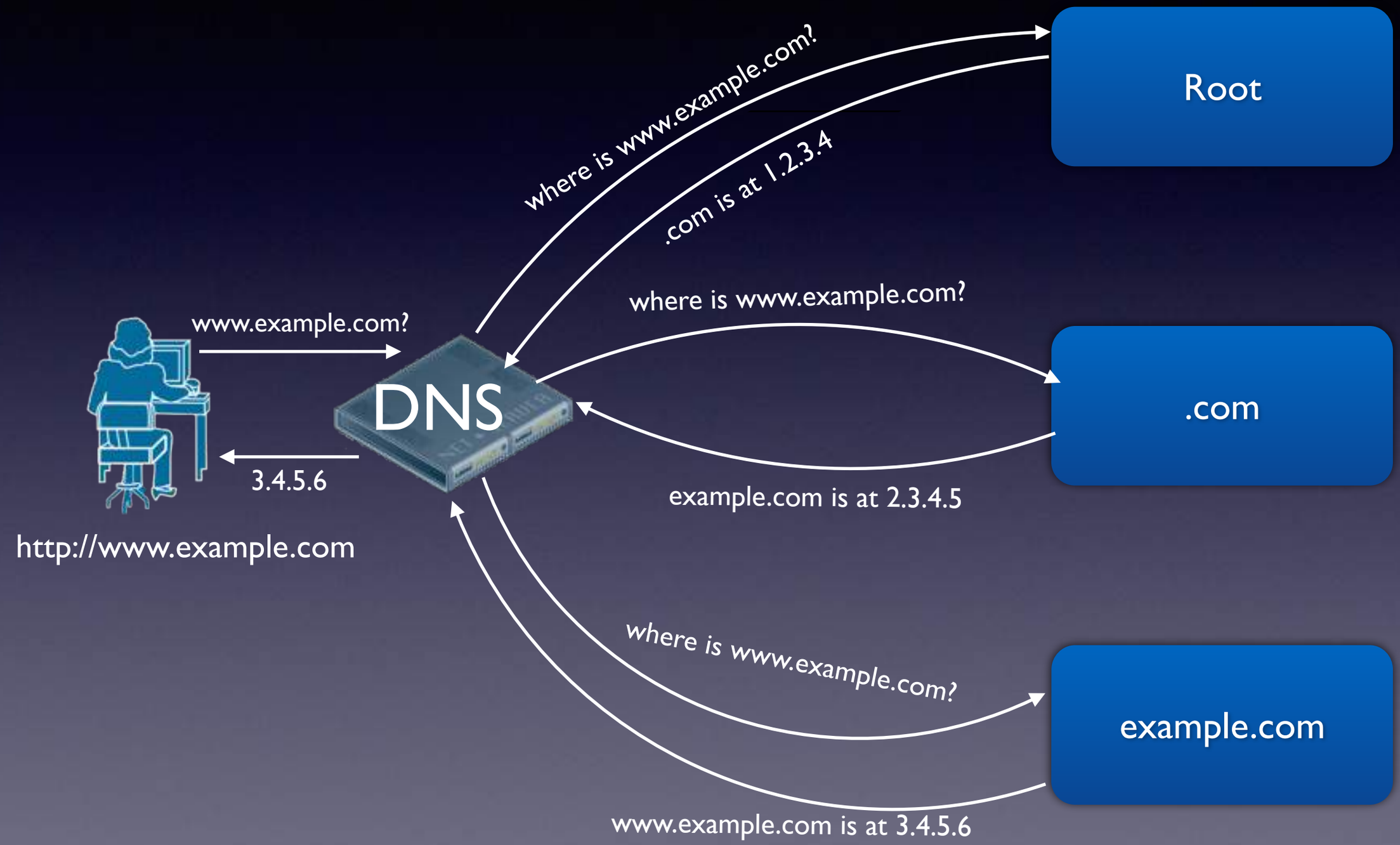
RFC 7258 - Pervasive Monitoring Is an Attack

The IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organisations. The IETF community has expressed strong agreement that PM is an attack that needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible.

How DNS works



How DNS *actually* works



So what?

- There is no need to ask the root the whole name — it only knows about TLDs
- There is no need to ask the .com servers about www.example.com — it only knows things directly in .com
- Asking the full question at each level means you are leaking information to the root and intermediate name servers.
- This is a short example, what about e.g. www.swiss.csail.mit.edu? www.hrc.org? www.aidshealth.org?

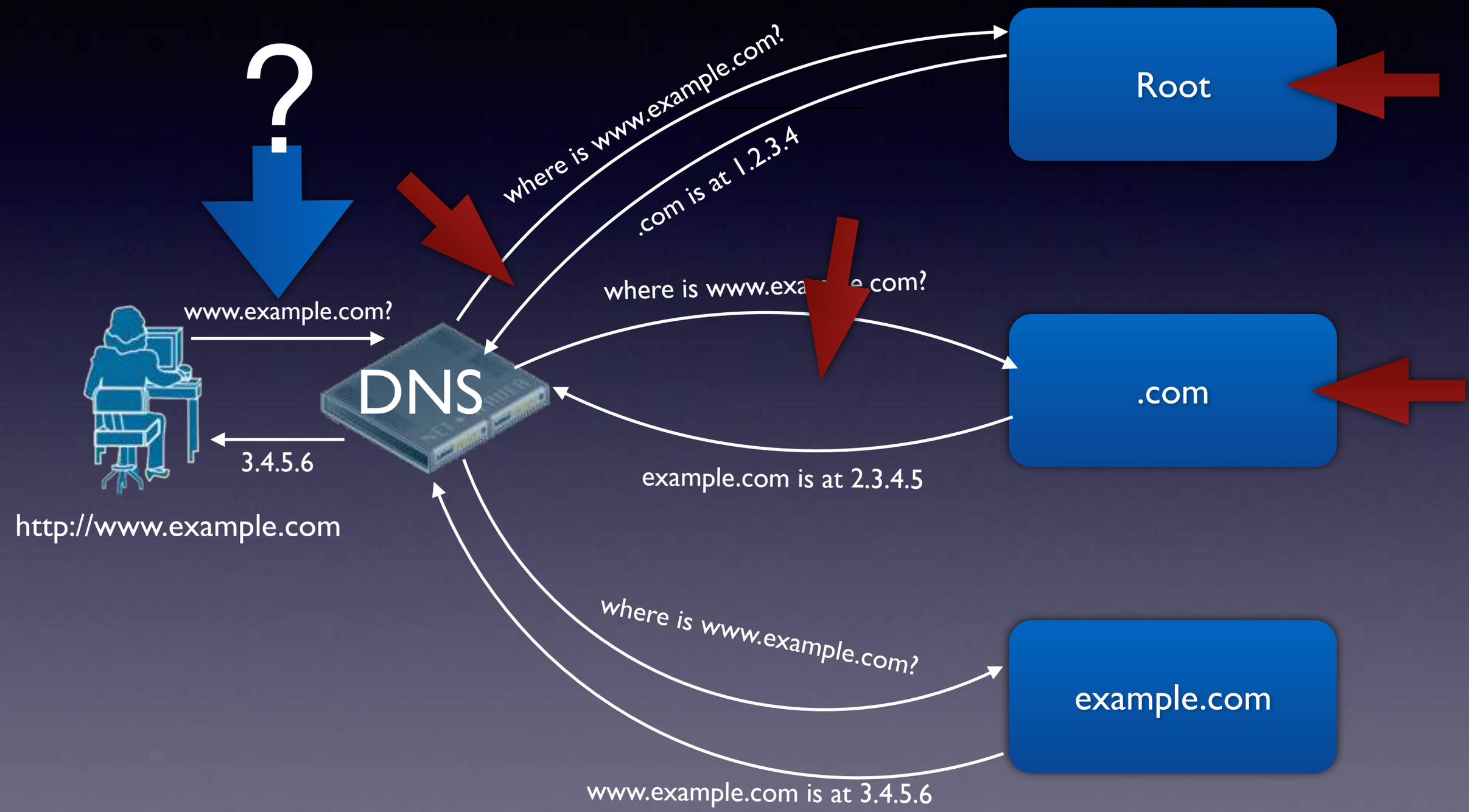
QNAME Minimization

- Really short summary is that it makes the behavior be how people describe it…
  - Only include .com when querying the root, only include example.com when querying .com, etc.
- Basically send the very minimum info needed to resolve the name.

QNAME Minimization

Pros	Cons
Privacy	Decrease in monitoring / statistics
Privacy	Sometimes additional lookups

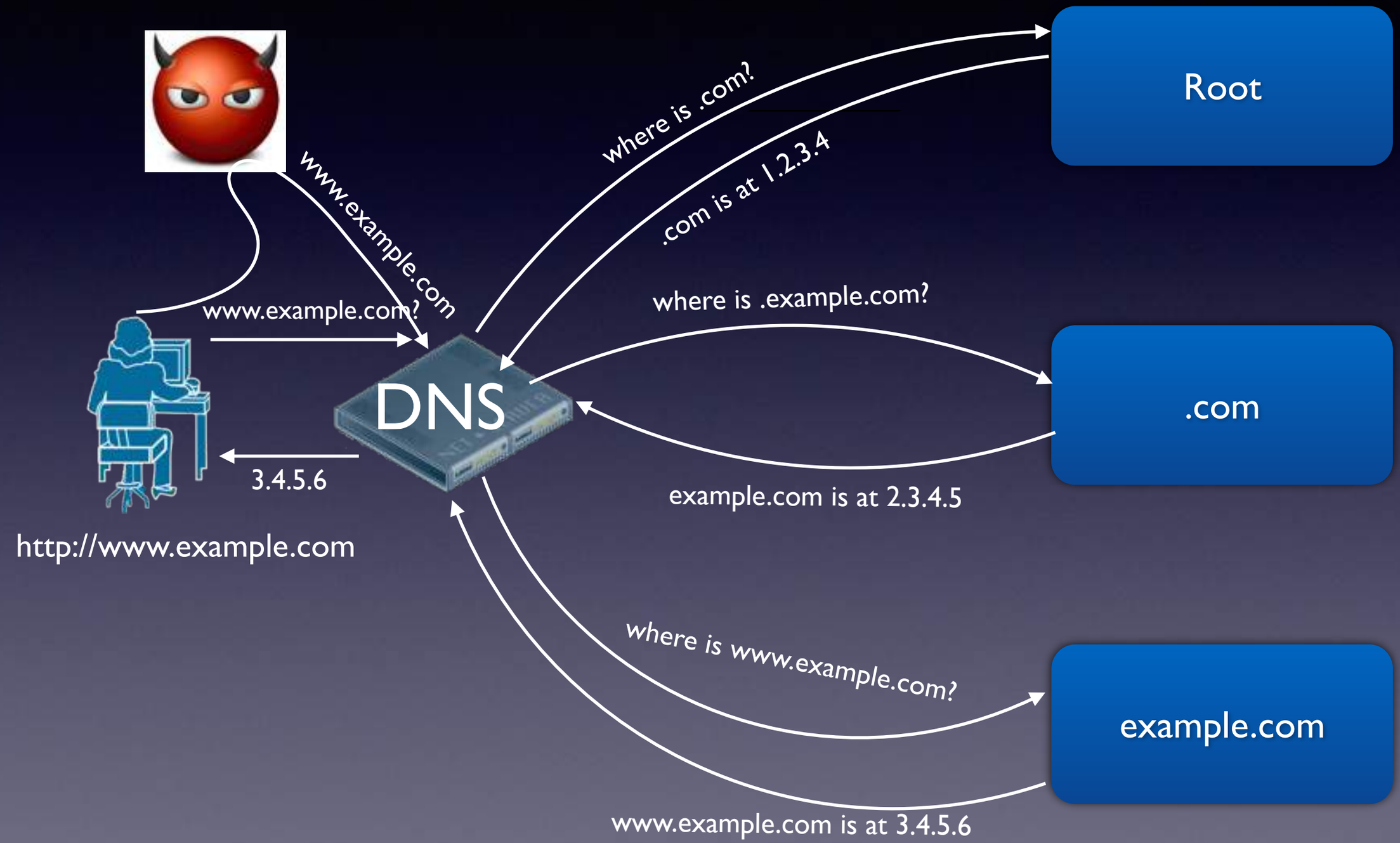
QNAME attack surface



DPRIVE WG

- This takes DNS privacy even further
  - Encrypts the DNS messages themselves
  - Addresses much more active attacks
  - Complements QNAME minimization
- New Working Group in the IETF

DPRIVE


Root
where is .com?
.com is at 1.2.3.4
www.example.com
www.example.com?
where is .example.com?
DNS
.com
3.4.5.6
example.com is at 2.3.4.5
http://www.example.com
where is www.example.com?
example.com
www.example.com is at 3.4.5.6

No Privacy

```
15:48:29 IP 204.42.252.2.26838 > 199.19.53.1.53:
A? www.aa.org. ar: . OPT UDPsize=4096 OK
0x0000:45000043a40a00004011125ecc2afc02  E..C….@..^.*..
0x0010:c713350168d60035002fc48293110000  ..5.h.5./......
0x0020:0001000000000001037777702616103   .........www.aa.
0x0030:6f726700001000100002910000000080  org.......).....
0x0040:0000                              ...

15:48:29 IP 199.19.53.1.53 > 204.42.252.2.26838:
q: A? www.aa.org. 0/6/1 ns: aa.org. NS ns2.rackspace.com.,
aa.org. NS ns.rackspace.com.
0x0000:45000260414a000038117b01c7133501  E..`AJ..8.{...5.
0x0010:cc2afc02003568d6024c230093118000  .*…5h..L#…..
0x0020:0001000000060001037777702616103   .........www.aa.
0x0030:6f726700001000100000200010001     org.............
```

With DPRIVE

```
15:59:51 IP 204.42.252.2.42607 > 185.49.141.38.1021
0x0000:4500015bc9b040000400066167cc2afc02  E..[..@.@.ag.*..
0x0010:b9318d26a66f03fdda34fe90e31ee965  .1.&.o…4.....e
0x0020:801800e50fd300000101080a783c373e  ..........x<7>
0x0030:d637f74516030101220100011e0303d6  .7.E....".....
0x0040:62f0d139ed30428d51e9802bfc89376e  b..9.0B.Q..+..7n
0x0050:09ddacbe0a20d6a5af716a70f9d6ea00  .........qjp....
0x0060:0088c030c02cc028c024c014c00a00a3  ...0.,.(.$......
0x0070:009f006b006a003900380088007c032   ...k.j.9.8.....2
0x0080:c02ec02ac026c00fc005009d003d0035  ...*.&.......=5
0x0090:0084c012c008001600013c00dc003000a  ..............
0x00a0:c02fc02bc027c023c013c00900a2009e  ./.+.'.#........
```

DPRIVE and ICANN

- Initially we are focused on encrypting from the client to the recursive server.
  - Impact recursive server operators - increased load from TCP / encryption
- Second phase - encrypting from the recursive to the auth server.
  - Impact to recursive and authoritative server operators - more TCP, encryption.

Questions?