Captive Portals, DPRIVE

Warren Kumari

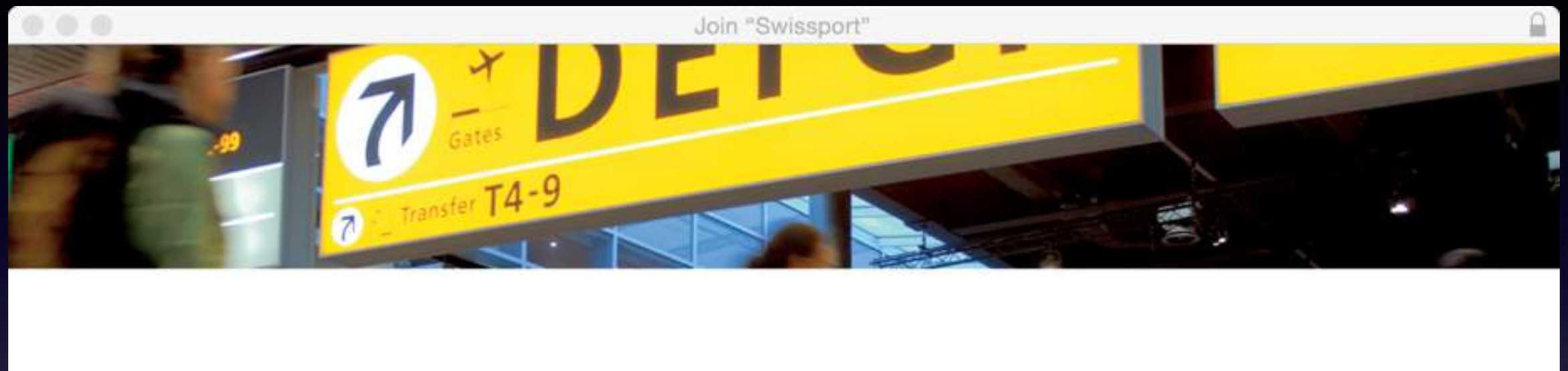
Captive Portals

- Controls access to a network until payment or AUP acknowledged.
- If you've ever visited a hotel, coffee shop, bookstore, airport, etc you've seen one of these.
- Annoying, but they seem to be here to stay.

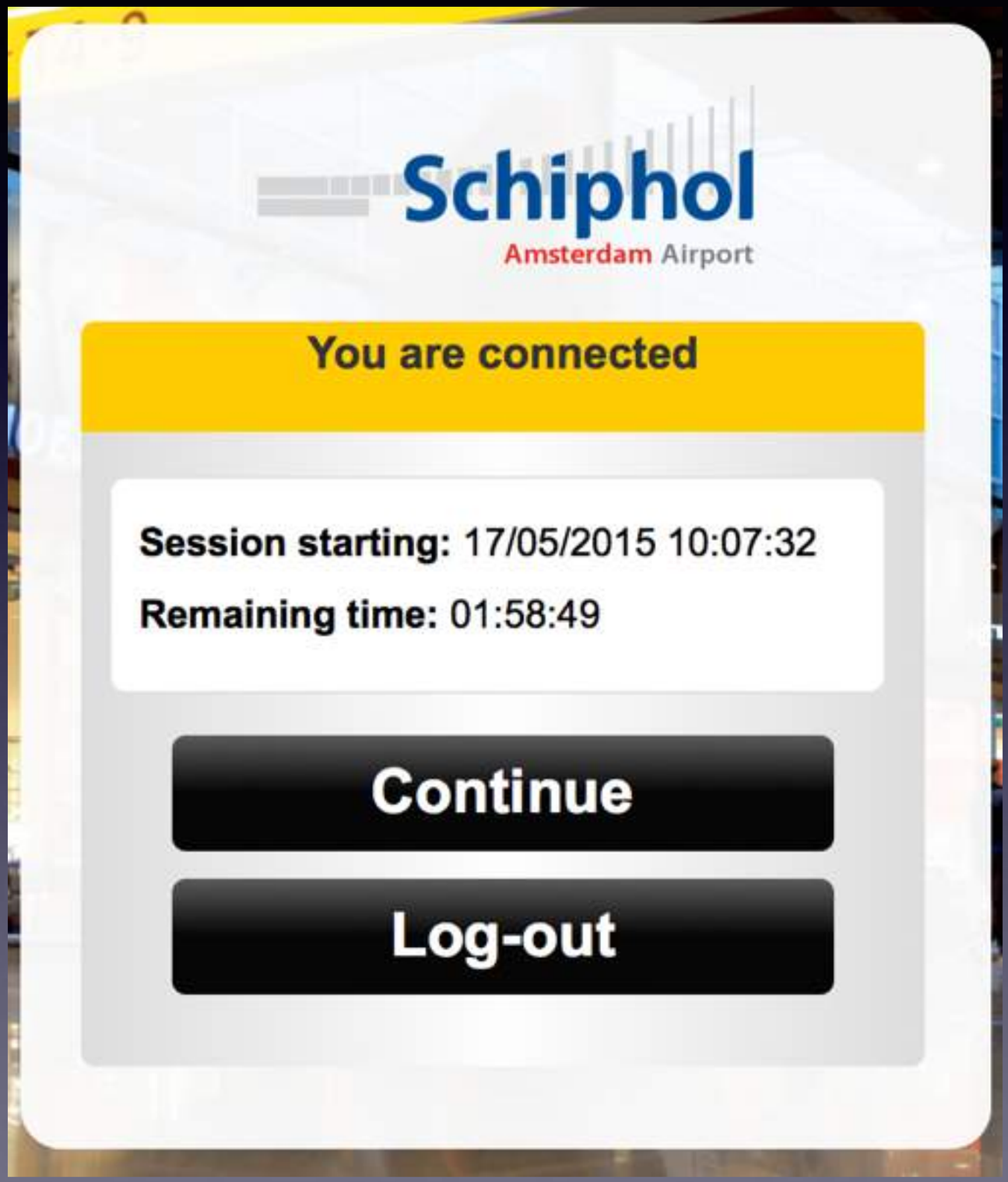
Issues

- Interception techniques
  - Unreliable
  - All look like MITM attacks
- Needs a web browser
- Hard to know what the status is

Captive Portal



Captive Portal



DNS Interception

- Either with site DNS servers (DHCP) or intercepting port 53
  - Breaks in the presence of DNSSEC
  - Breaks in a DPRIVE'd world
- Mucks up some applications
  - Apps call `gethostbyname()` once.
- Breaks if there is a VPN
- Breaks if there is a web proxy

HTTP Interception

- Requires that the user is going to HTTP site
  - Breaks if the user only uses HTTPS
- Breaks if there is HSTS
- Mucks up some applications
  - Many other apps use port 80…
- Breaks if there is a VPN or web proxy

HTTPS Interception

- Ugh.
- Breaks most things
- Teaches bad behavior
- Leaks credentials
- Interacts badly with many applications

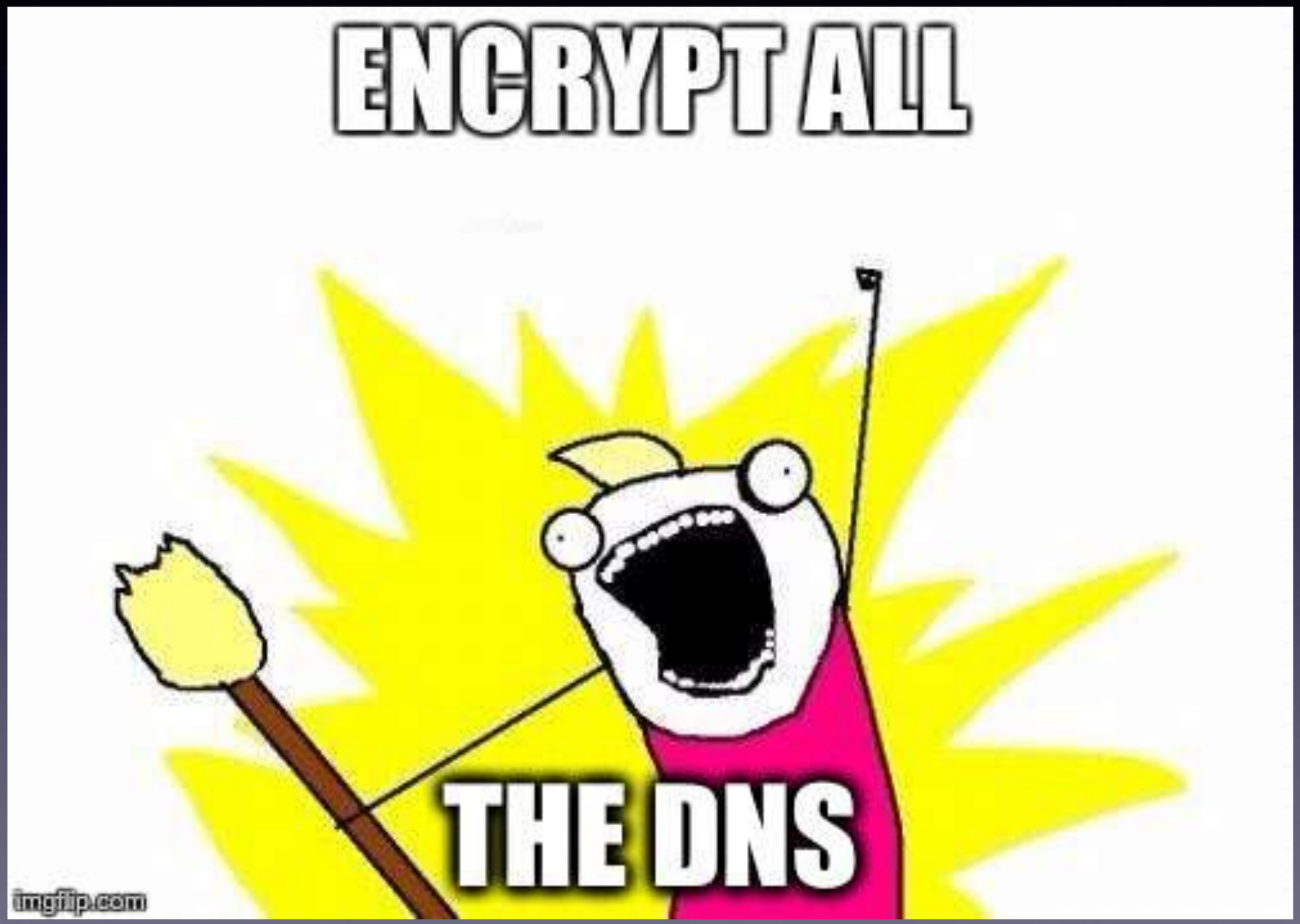
IP Interception

- Policy routes 0/0 to the CP box
- CP pretends to ran services on all addresses
- Same issues as above

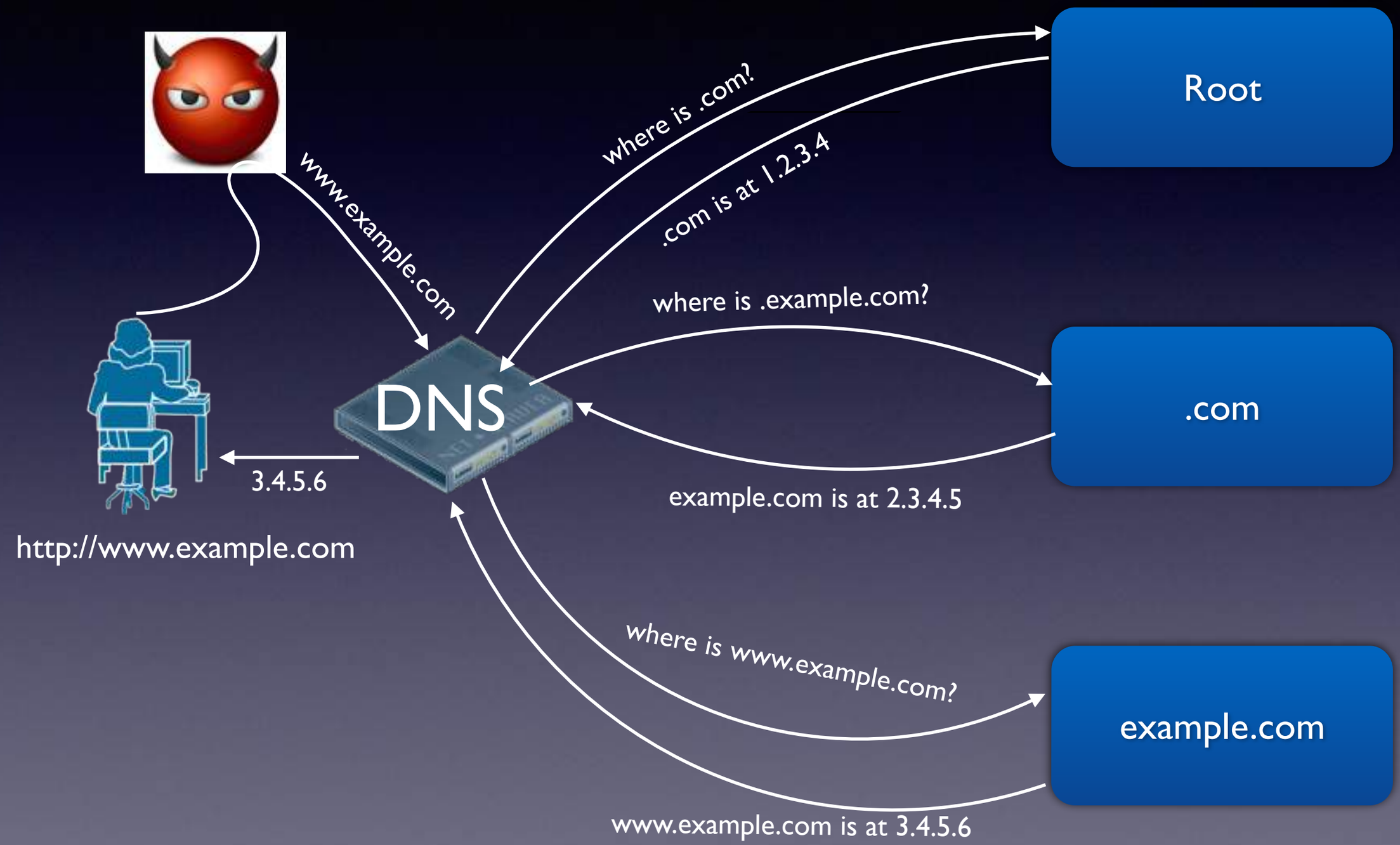
Solutions?

- IETF CAPPORT WG.
  - BarBoF in Dalls
  - Real BoF in Prague
    - Charter
      - Working on captive portal discovery and interaction.
- `draft-wkumari-dhc-capport`
  - AD sponsored

DPRIVE WG



DPRIVE


Root
where is .com?
.com is at 1.2.3.4
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

Status

- 2 phases
  - Encrypt from Stub to recursive
    - Recursive to auth.
- Agreed on primary document / design
- Adopted, working on documents
- Working toy implementations

Status

- `draft-ietf-dprive-problem-statement`
  - IETF LC
- `draft-ietf-dprive-start-tls-for-dns`
  - DNS over TLS over TCP
- `draft-ietf-dprive-dnsodtls`
  - DNS over DTLS over UDP

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  ./.+.'.#........
```

Questions?