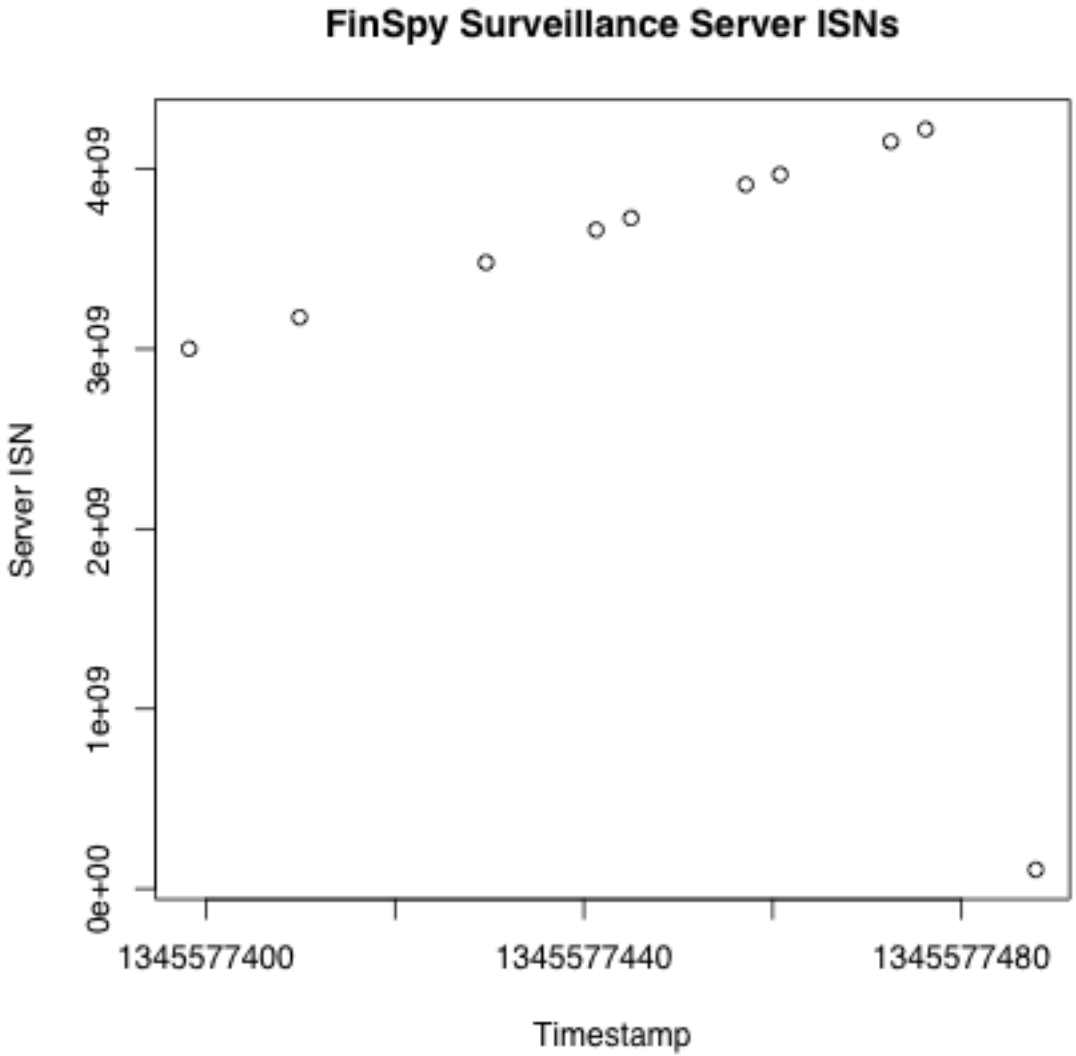
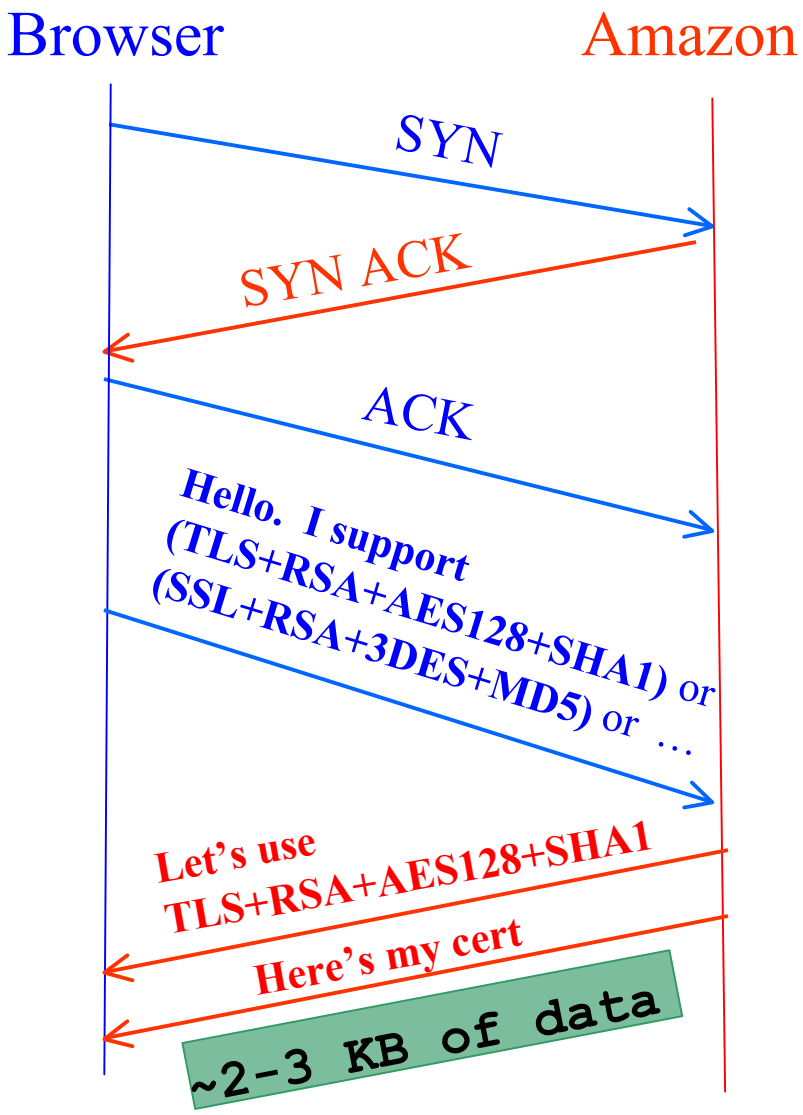
reason	occurences
NULL	921683
Affiliation Changed	41438
CA Compromise	248
Certificate Hold	80371
Cessation Of Operation	690905
Key Compromise	73345
Privilege Withdrawn	4622
Superseded	81021
Unspecified	168993

https://www.eff.org/deeplinks/2011/10/how-secure-https-today


FinSpy Surveillance Server ISNs
Server ISN
0e+00
1e+09
2e+09
3e+09
4e+09
1345577400
1345577440
1345577480
Timestamp

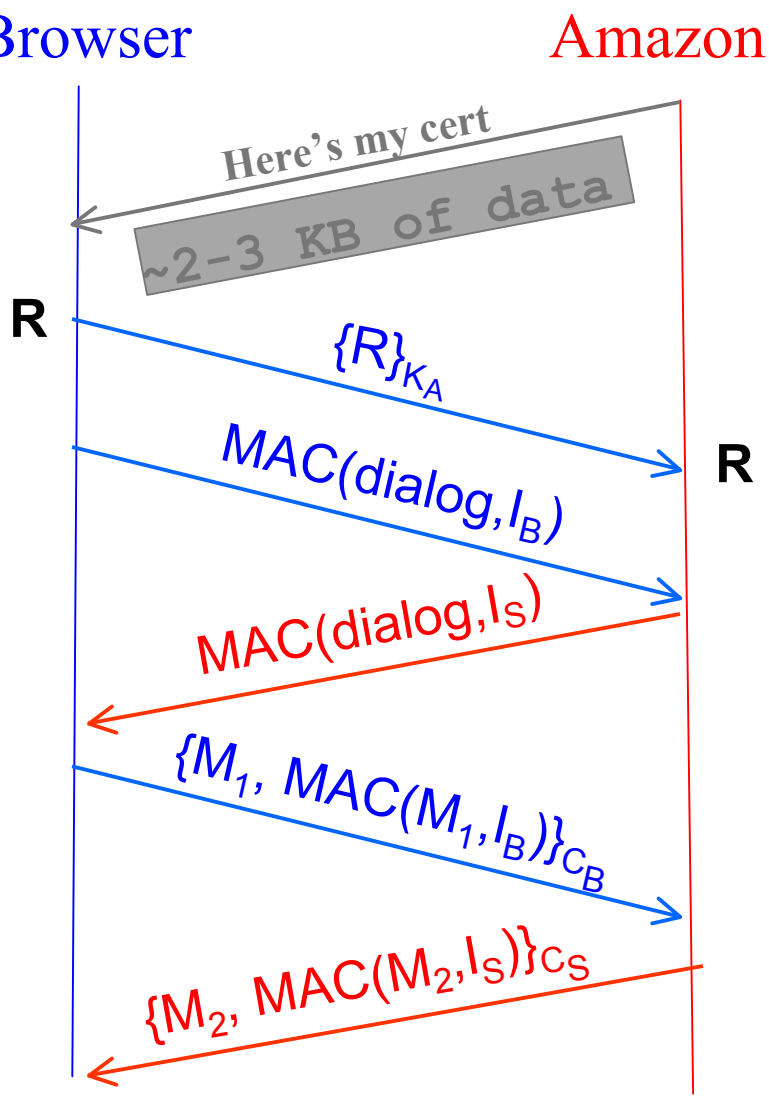
`HTTPS` Connection (SSL / TLS)

- Browser (client) connects via TCP to Amazon's **`HTTPS`** server
- Client sends over list of crypto protocols it supports
- Server picks protocols to use for this session
- Server sends over its certificate
- (all of this is in the clear)
- ***Client now validates cert***

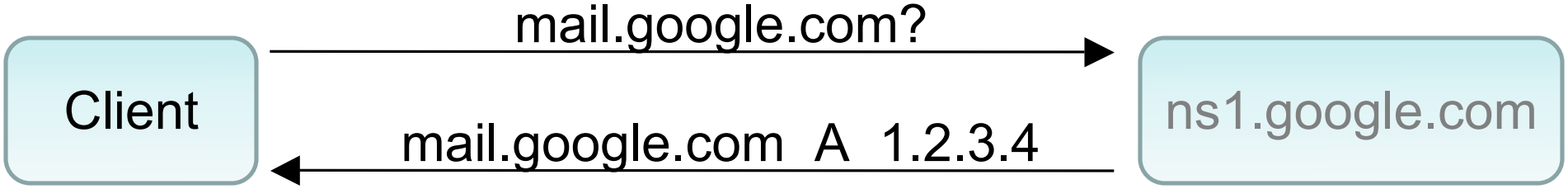


HTTPS Connection (SSL / TLS), con't

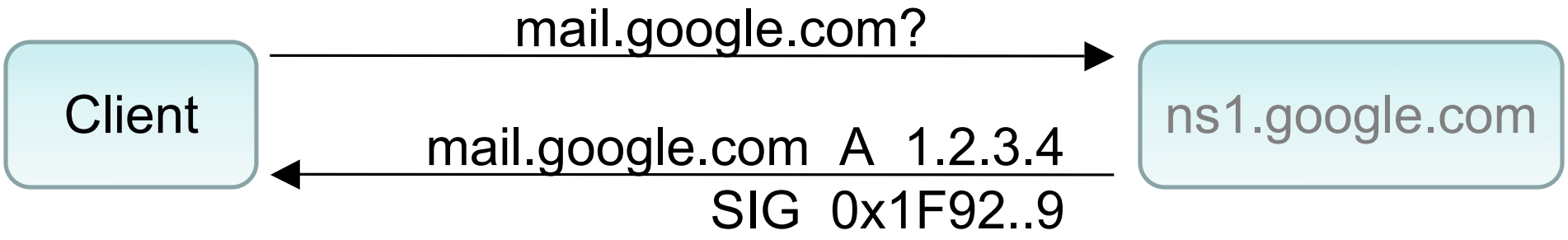
- For RSA, browser constructs a long (2048 bits) random string R
- Browser sends R encrypted using Amazon's public RSA key K_A
- From R browser & server derive pairs of symm. *cipher keys* (C_B, C_S) and MAC *integrity keys* (I_B, I_S)
  - One pair to use in each direction
- Browser & server exchange MACs computed over entire dialog so far
- If good MAC, Browser displays 
- All subsequent communication encrypted w/ symmetric cipher (e.g., AES128) cipher keys, MACs
  - Messages also numbered to thwart replay attacks

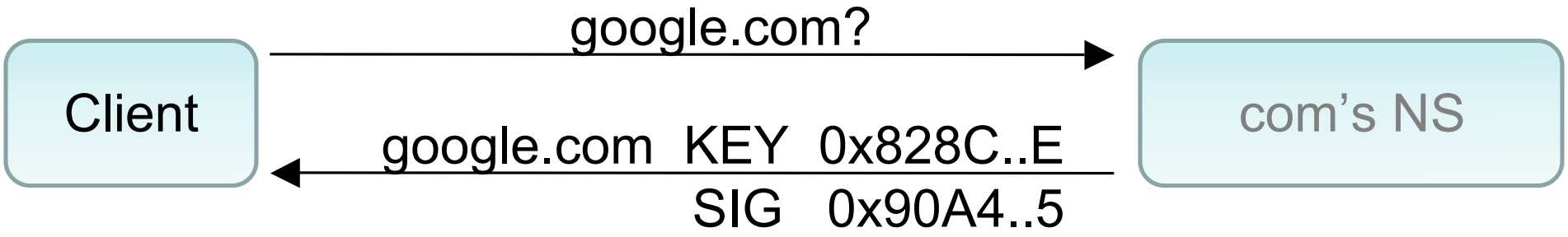


Ordinary DNS:



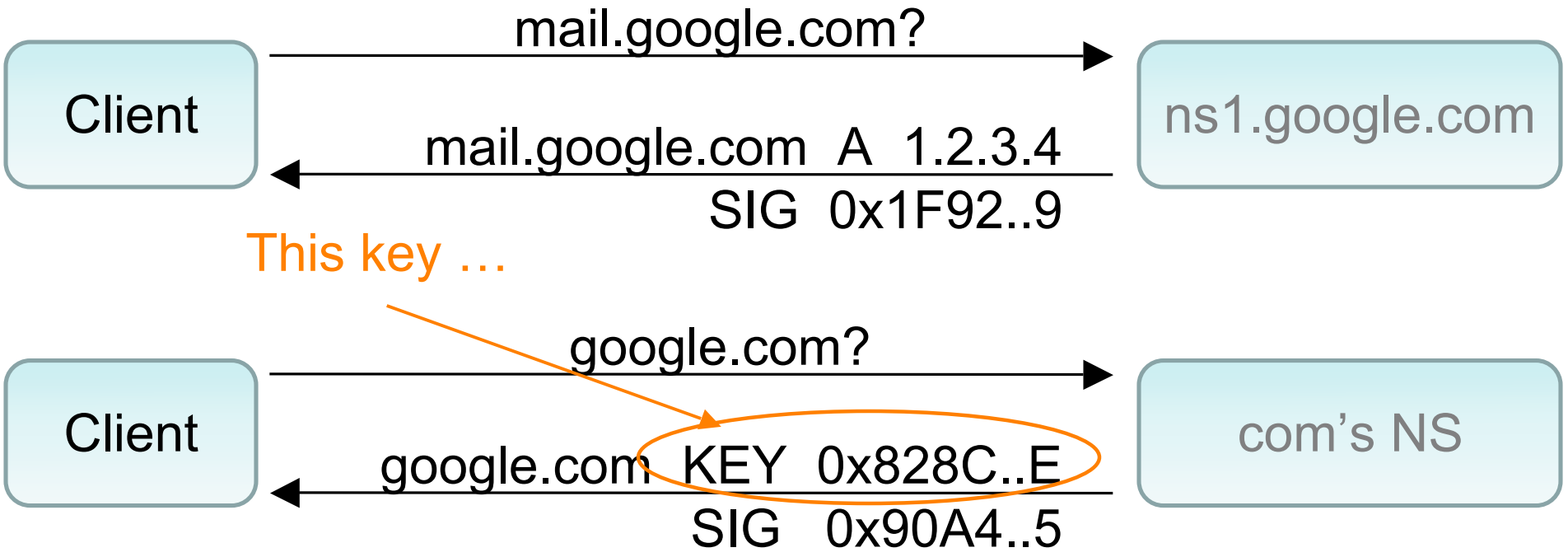
DNSSEC:





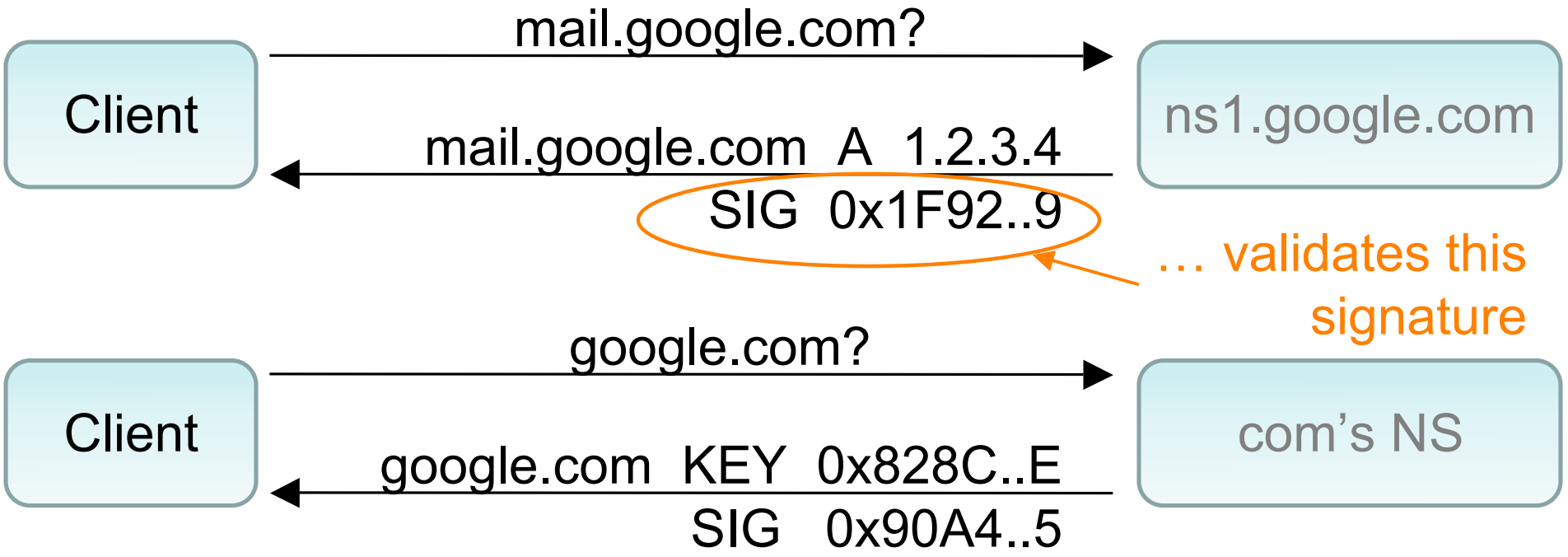
Ordinary DNS:

DNSSEC:



Ordinary DNS:

DNSSEC:



Ordinary DNS:

DNSSEC: