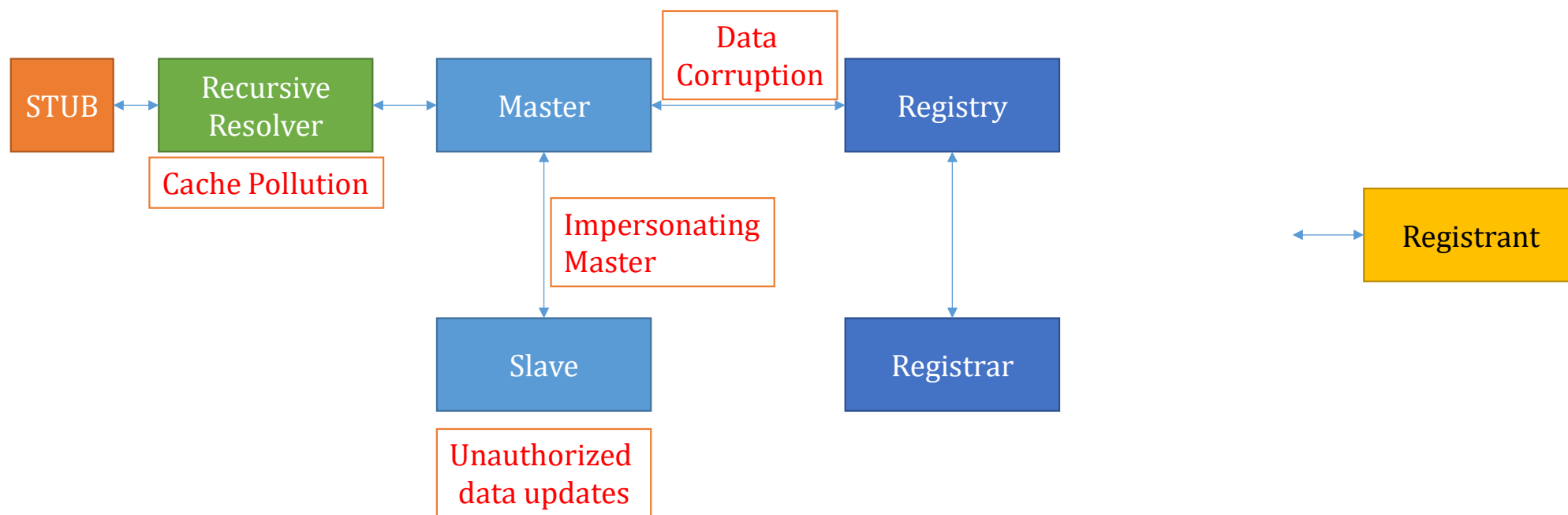


# DNS Security & Privacy

Anoop Kumar Pandey  
Principal Technical Officer  
Centre for Development of Advanced Computing (C-DAC)  
Electronics City, Bangalore 560 100

Centre of Excellence in DNS Security  
23<sup>rd</sup> December 2021

# DNS Infrastructure Attack Landscape



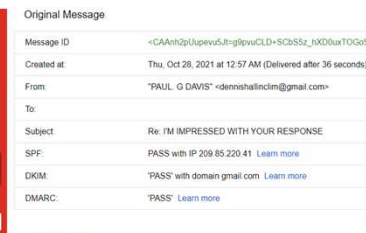
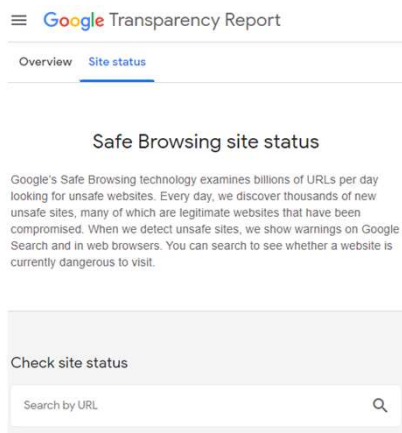
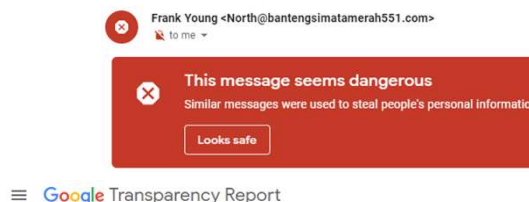
\*MiTM between each entity

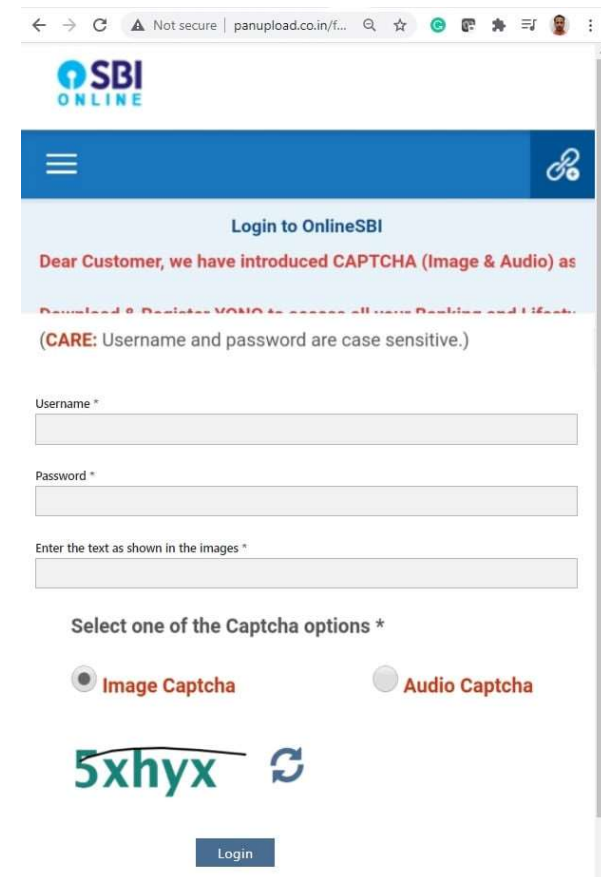
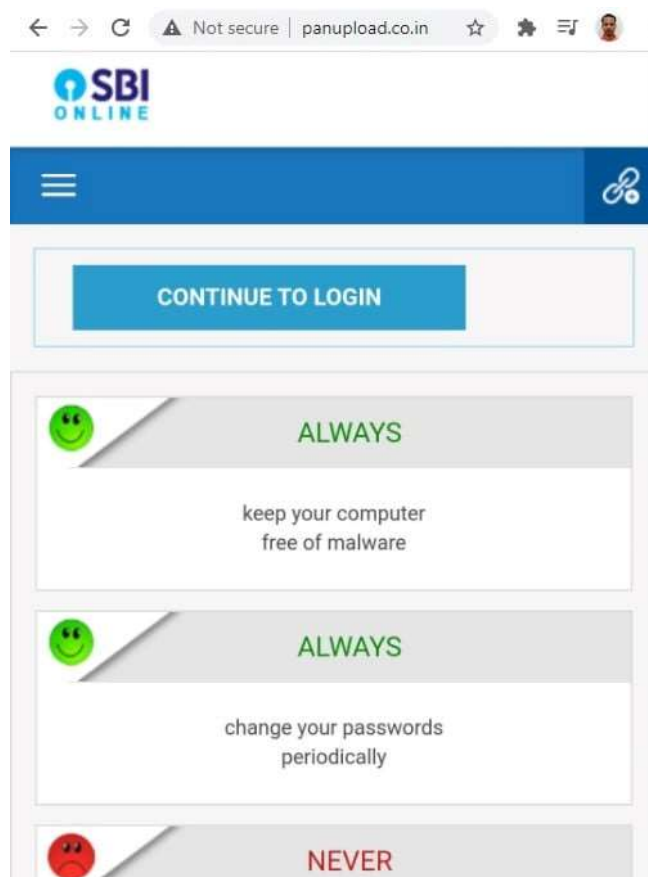
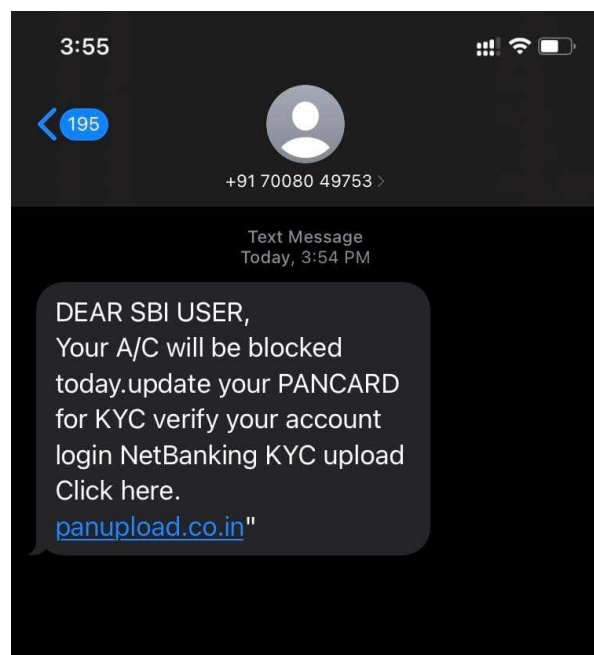
\*DNS Software Vulnerability wherever applicable

Disrupt DNS = Disrupt Internet  
= Disrupt Service

- Whois data
  - Recent domain registration creation date
  - Questionable Whois contact data
  - Privacy protection service
- Email
  - Show Original
  - Name & Email
- URL check
  - Brand misuse
  - Long URL, base site absent
- TLS Certificate check
- Suspicious host, operator, NS
- Safe Browsing Check
- URL Filter
- Tools like nslookup, dig

```
Domain Name: coednssecurity.in
Registry Domain ID: D41440000006446126-IN
Registrar WHOIS Server:
Registrar URL: https://publicdomainregistry.com/
Updated Date: 2018-10-02T19:21:38Z
Creation Date: 2018-08-03T11:20:57Z
Registry Expiry Date: 2028-08-03T11:20:57Z
Registrar: Endurance Digital Domain Technology LLP
Registrar IANA ID: 801217
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Centre for Development of Advanced
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Karnataka
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
```



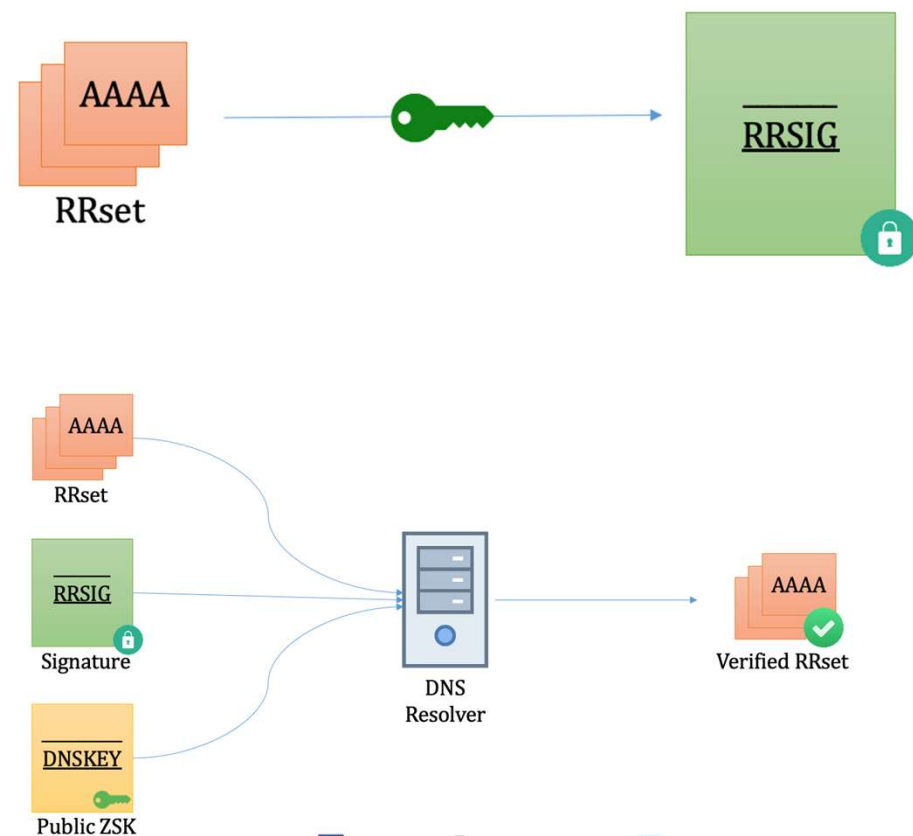


# Some Remedies

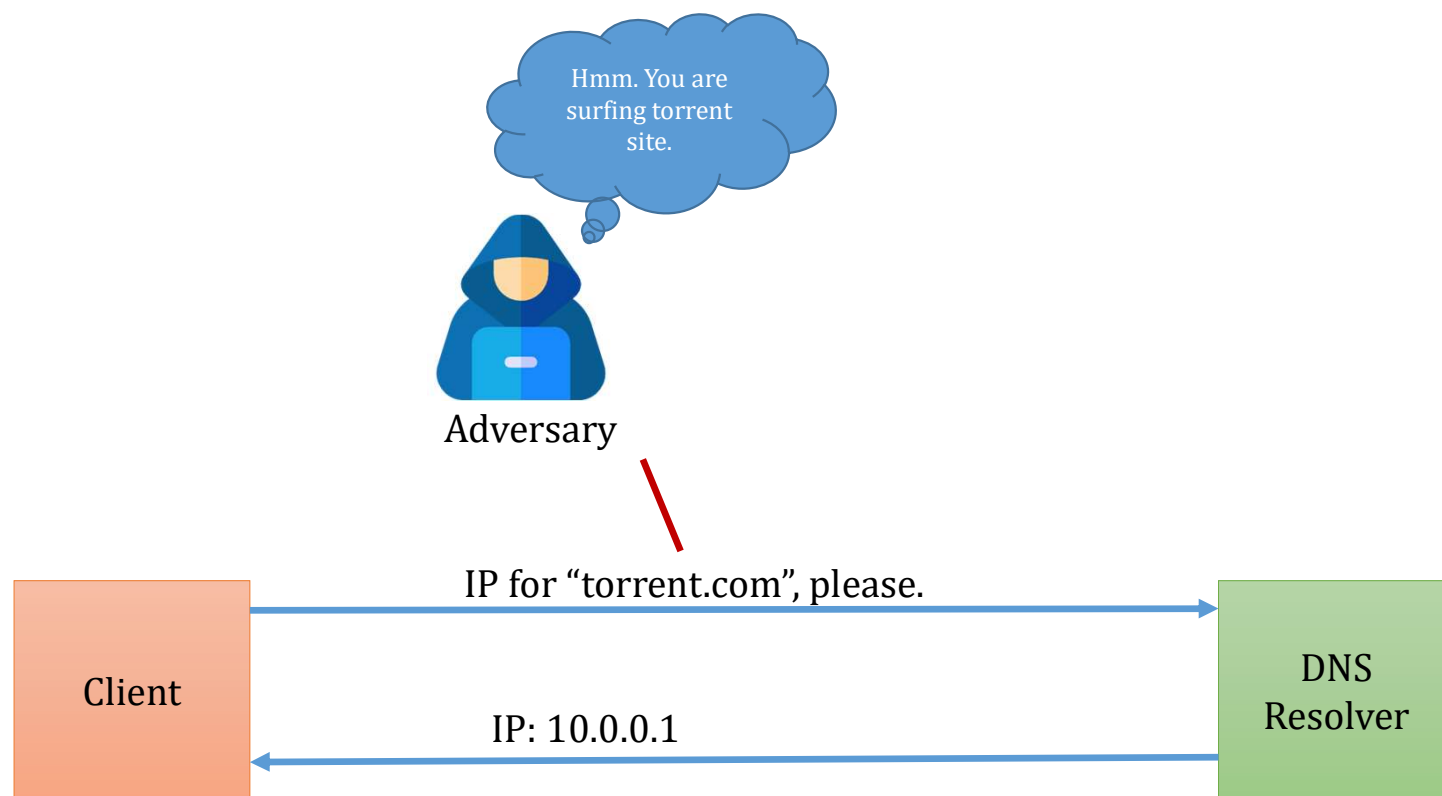
- DNSSEC
- Mail Exchanger Security: SPF, DKIM
- Awareness: DNS Tools, Modus Operandi
- Open DNS Resolver
  - Configure well!
- Scam: Don't believe too much on your luck
- End Point Protection
- Report

# DNSSEC

- Adds a layer of Trust through authentication
  - Adds cryptographic signature to existing DNS Records
- Verify Signature
  - Data coming from authoritative server
  - Ensures
    - No modification en-route
    - No fake record injection
- Trust Propagation
- DNSSEC Guarantees:
  - Authenticity of DNS answer origin
  - Integrity of reply
  - Authenticity of denial of existence
- DNSSEC does not
  - Provide confidentiality for DNS data
  - Protect against Denial of Data

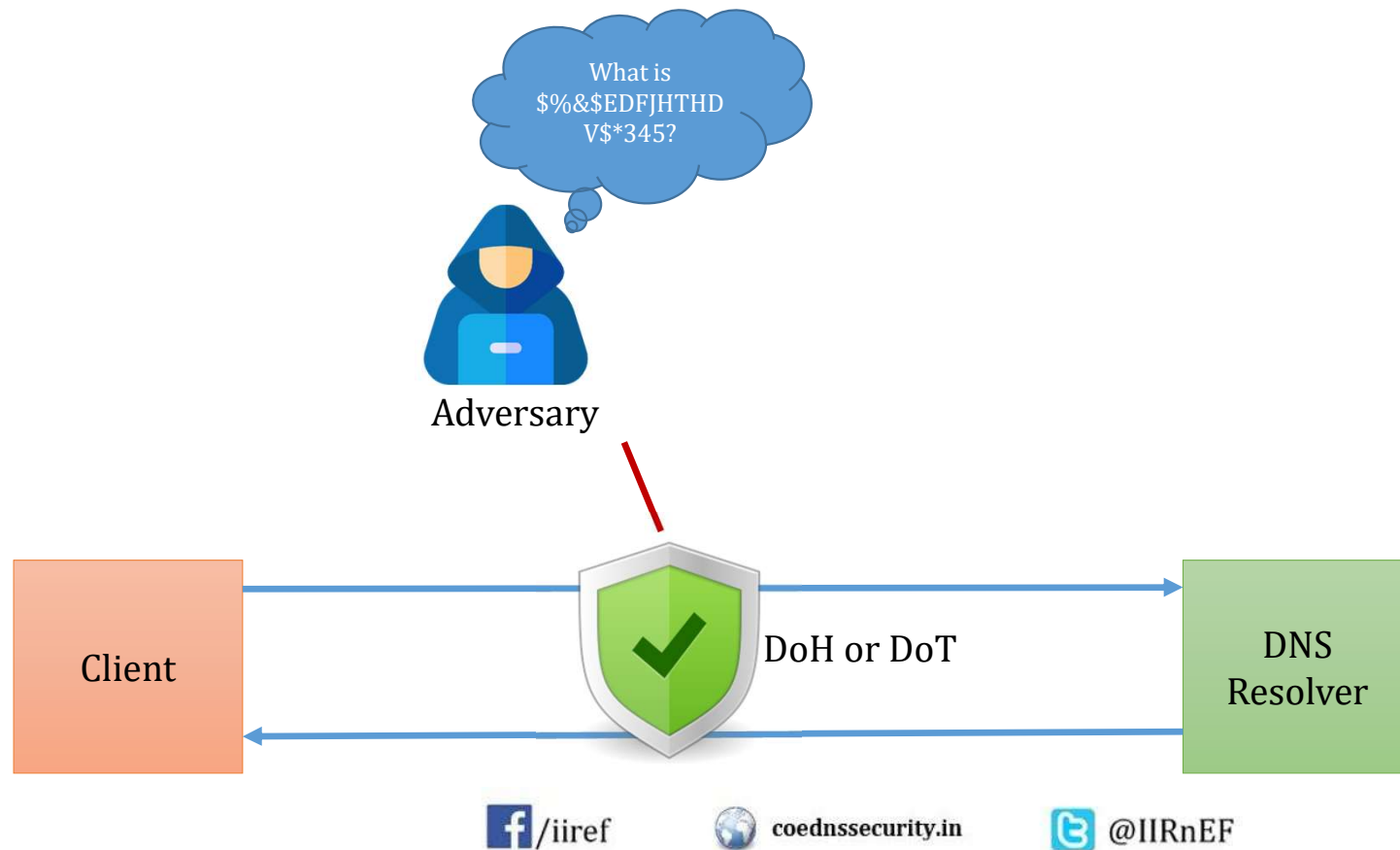


# Need for Encrypted DNS Query





# Encrypted DNS Traffic



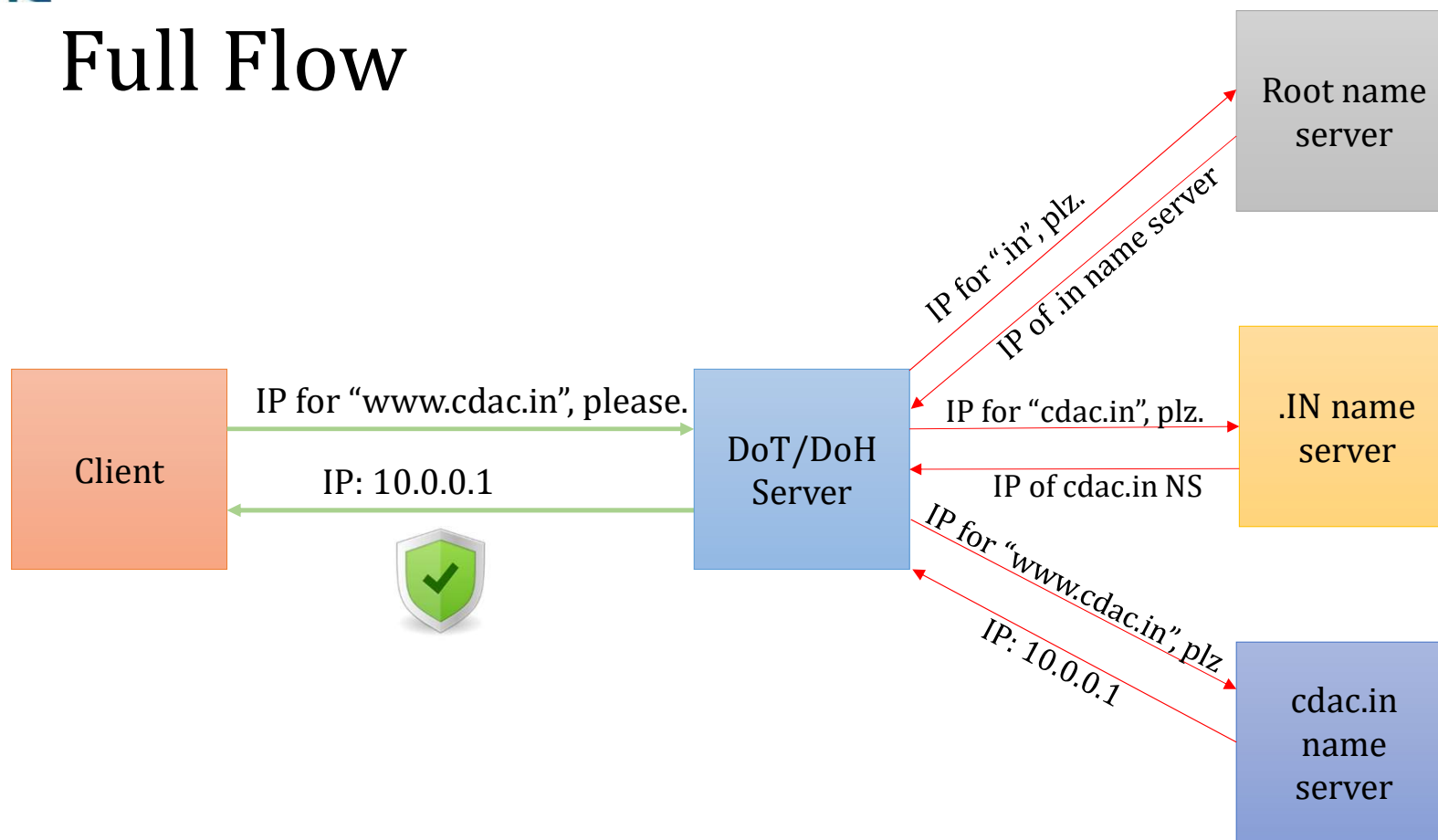
# DNS over TLS (DoT)

- TLS Encryption on top of UDP
- Detailed in RFC 7858 (<https://tools.ietf.org/html/rfc7858>)
- Safeguard from MiTM
- Client doesn't query Authoritative Sever, rather DoT server makes traditional recursive queries.
- Default Port: 853
- Support
  - Android 9+
  - iOS 14+
  - Windows/Linux through packages

# DNS over HTTPS (DoH)

- DNS Queries sent over HTTPS
- Request/Response in JSON format, GET/POST
- Port: 443
- Detailed in RFC 8484 (<https://tools.ietf.org/html/rfc8484>)
- Client doesn't query Authoritative Server, rather DoH server makes traditional recursive queries.
- Support
  - Android 9+
  - iOS 14+
  - Windows, Linux (coming soon)
  - Firefox (working), others (intermittently)
- Server Examples
  - dns.google
  - cloudflare-dns.com

# Full Flow



# Thank You