DNS Security from the Client Perspective

What is DNS?

- DNS is the Domain Name System
  - human readable names like www.apnic.net
  - translated into addresses like 104.20.22.173 or 2606:4700:10::6814:24ad
- DNS is an old protocol
  - RFCs 882 and 883 were written in 1983 that cover what domain names are and how to implement them
    - RFC = “Request For Comments” which are internet standards documents
  - RFC1035 was written in 1987 which extended DNS to use TCP as well as UDP

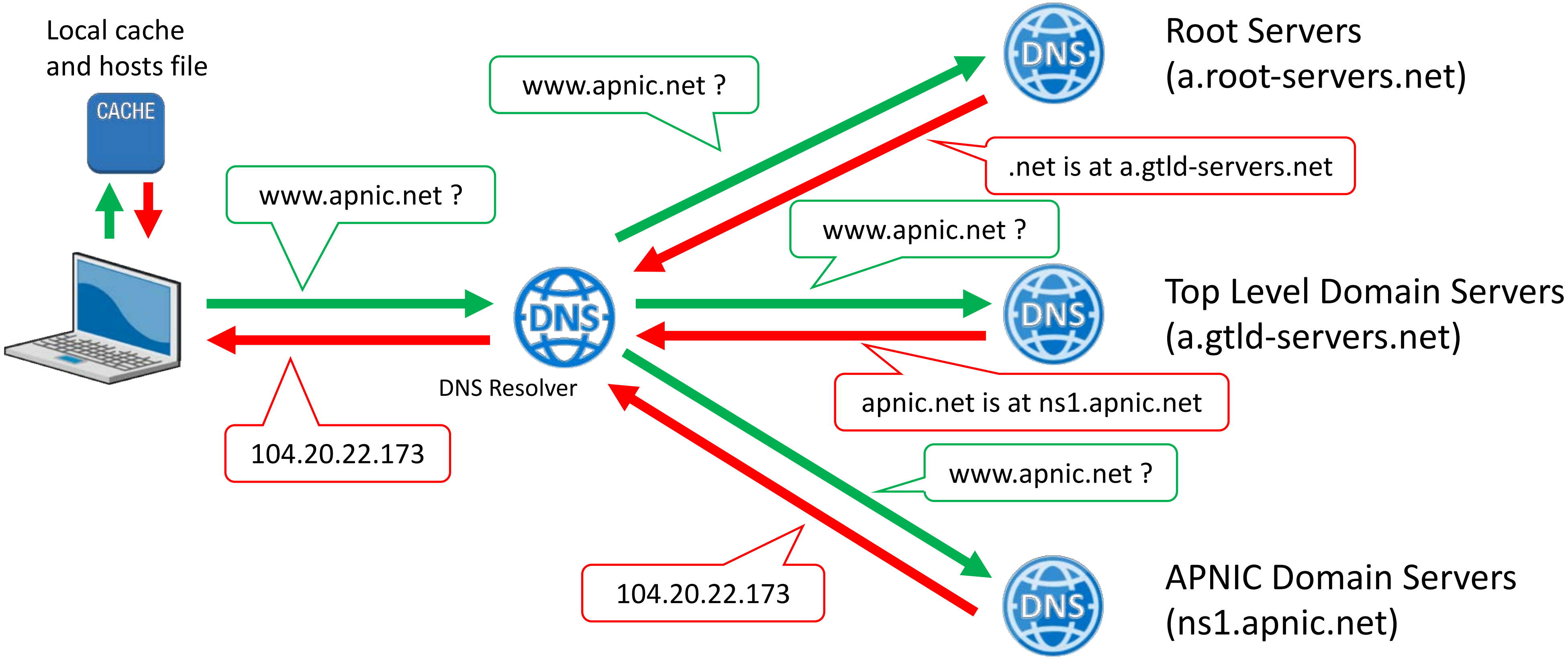
Life of a Domain Name

- The registrant (you) pays to register a domain with a registrar
  - Technically you don't buy a domain, more like renting
- The registrar checks with the appropriate registry database to see if the domain name is available
- The registrar then registers the domain with the registry and the registry configures the TLD root servers with the DNS server details you provided

Where Can Domain Names Go Wrong?

- Someone else may have already registered a domain:
  - With your company name
  - With a name similar to your company name
- If you don’t renew your domain name, it will expire
  - Someone else can pay to acquire your newly available domain name
  - There are entire businesses built to find and re-sell these expired domains
- Malicious attackers can break into your registrar account
  - Redirecting your entire domain to DNS servers controlled by the attacker
  - This is a supply chain risk
  - Does your domain registrar support 2FA?
  - Will your registrar make changes based on a FAX or letter on fake letterhead?

Life of a DNS Request



Local cache and hosts file

www.apnic.net ?

104.20.22.173

DNS Resolver

www.apnic.net ?

.net is at a.gtld-servers.net

www.apnic.net ?

apnic.net is at ns1.apnic.net

www.apnic.net ?

104.20.22.173

Root Servers (a.root-servers.net)

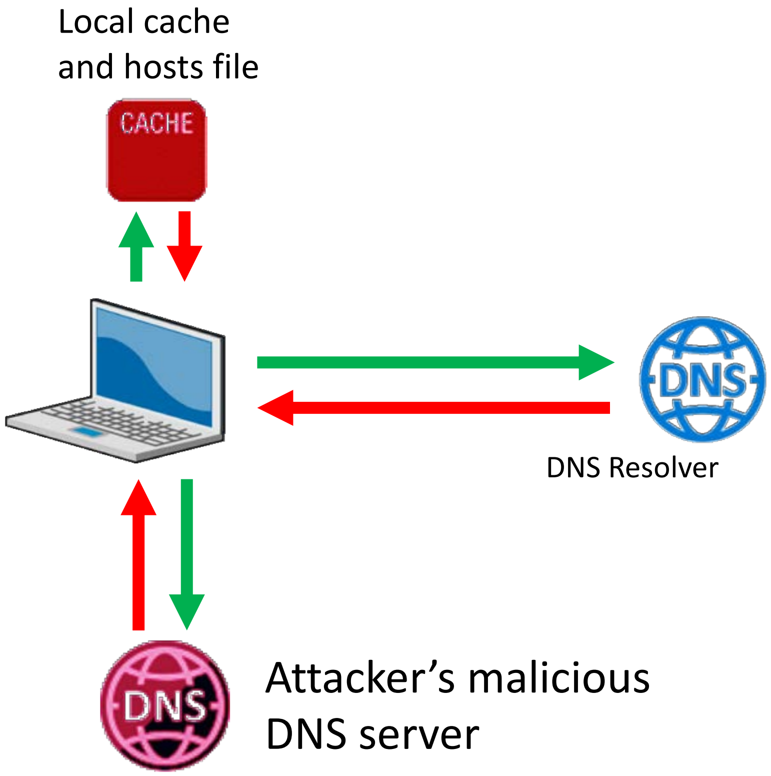
Top Level Domain Servers (a.gtld-servers.net)

APNIC Domain Servers (ns1.apnic.net)

Where Can DNS Go Wrong?

- Lots of ways!
- Let’s examine the security issues along each step of a DNS request
- Remember to identify security compromises against:
  - Confidentiality
  - Integrity
  - Availability

Problem – Local Hosts and Client Malware

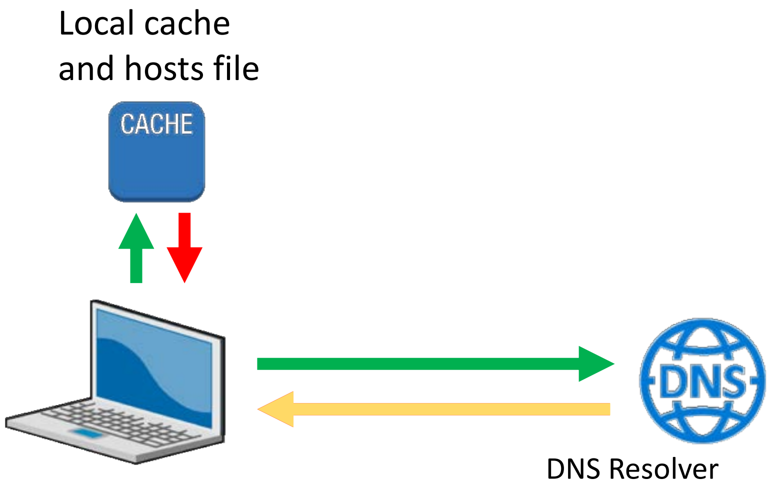


- Malware edits the local hosts file to answer the request before contacting a DNS resolver

or

- Malware changes local DNS settings to use an attacker's DNS server and return false responses

Problem – DNS Resolvers



- DNS Resolvers can be configured to modify responses
- Attackers can remotely poison DNS Resolvers to give false responses
- DNS Resolvers can block responses

Problem – Privacy Like A Postcard

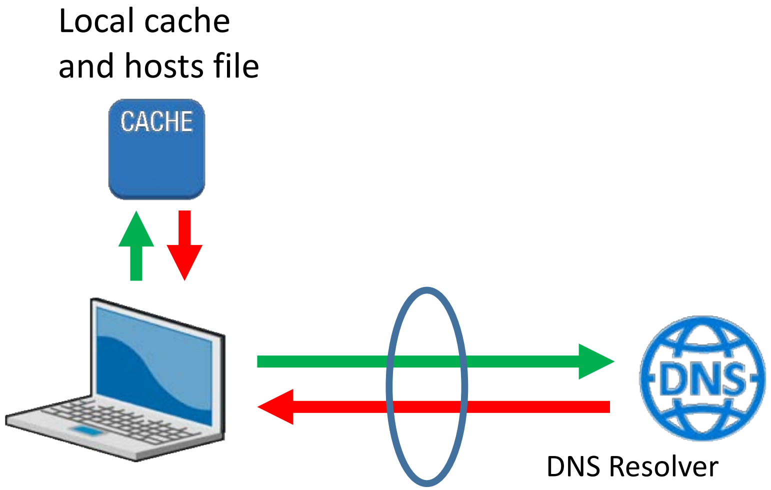
GRAVITY FALLS
MYSTERY SHACK
POST CARD

What is the IP
address for
www.apnic.net
???

To:
DNS Resolver

From:
My Laptop PC

Problem – Privacy Like A Postcard

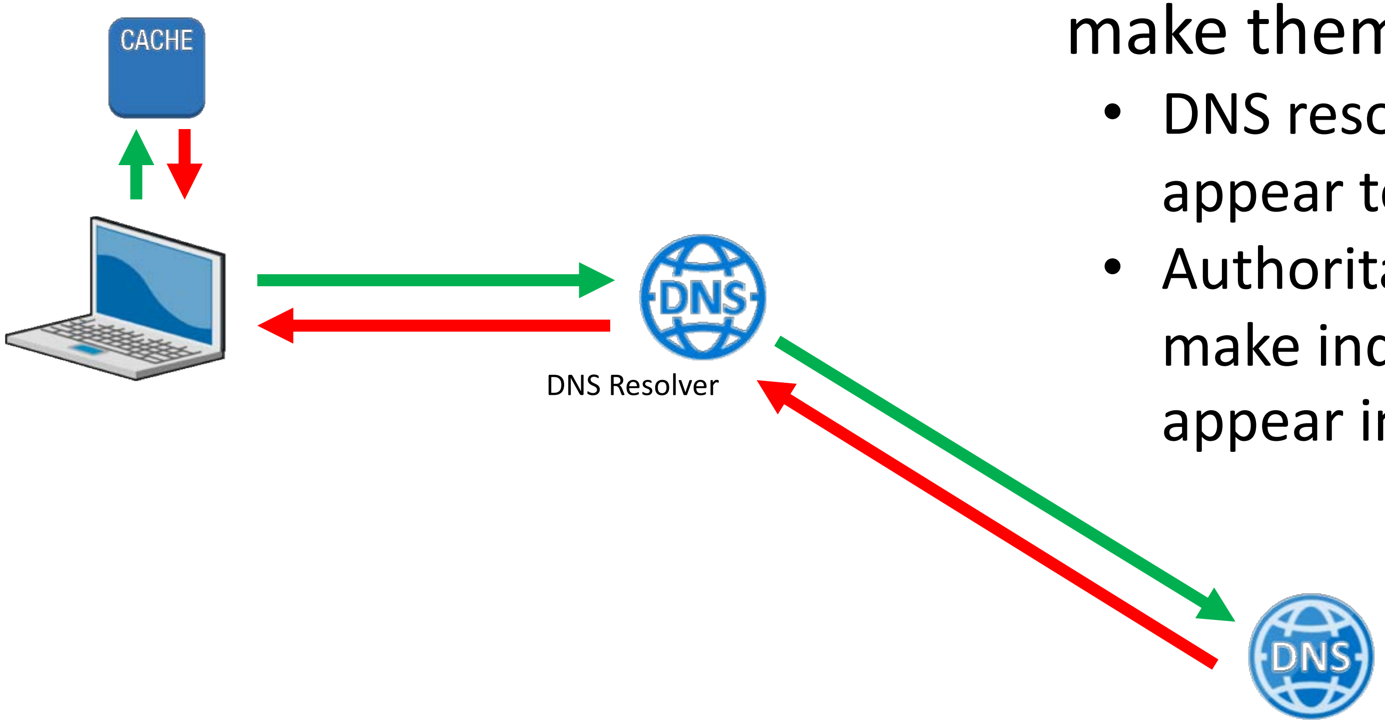


- DNS queries and responses are sent as unencrypted cleartext
- DNS queries and responses can be read and stored:
  - By the local network operator
  - By the upstream Internet provider

Problem – Denial of Service Attacks

- Distributed Denial of Service (DDoS) attacks can overwhelm servers and make them unresponsive
  - DNS resolver attacks make the internet appear to be inaccessible
  - Authoritative domain server attacks make individual domains and web sites appear inaccessible

Local cache
and hosts file



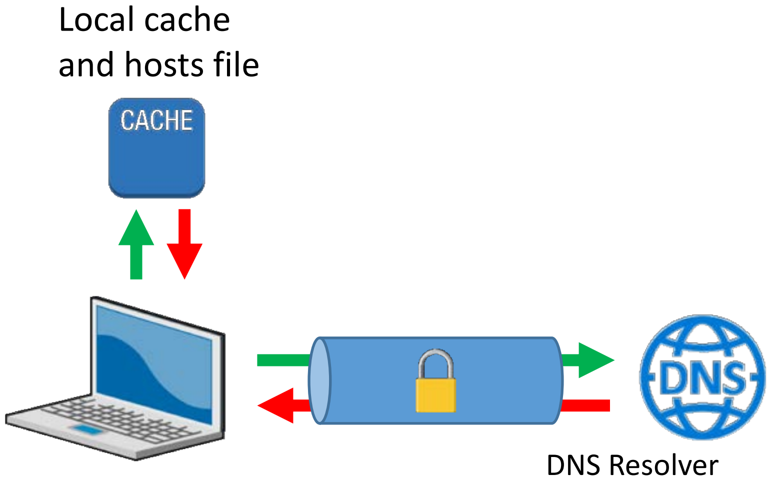
DNS Resolver

APNIC Domain Servers
(ns1.apnic.net)

Making DNS Secure

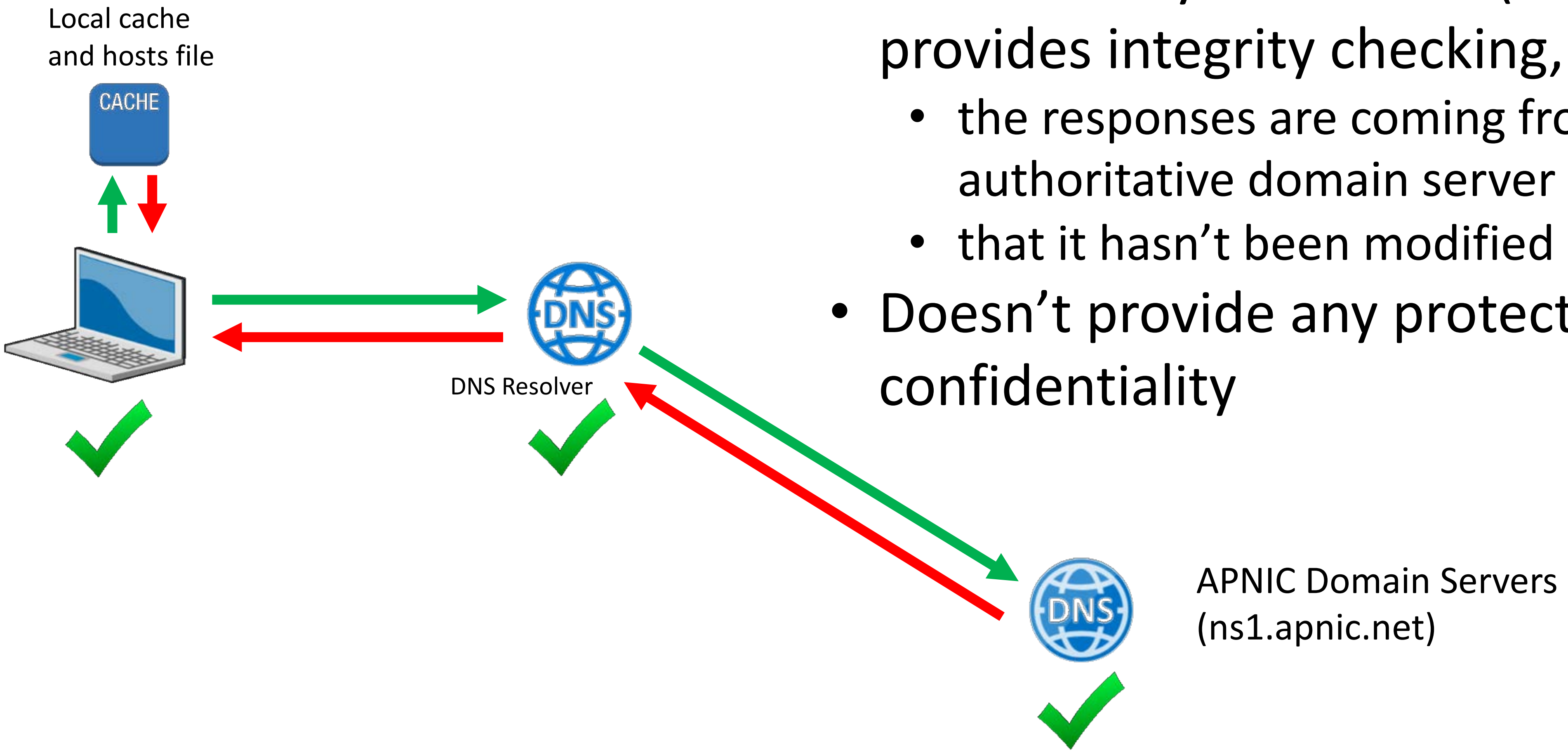
- Think back to the 3 concepts we want to protect and how can we defend them
  - Confidentiality
    - Encryption
  - Integrity
    - Cryptographic hash verification
  - Availability
    - Redundancy

Making DNS Secure - Encryption



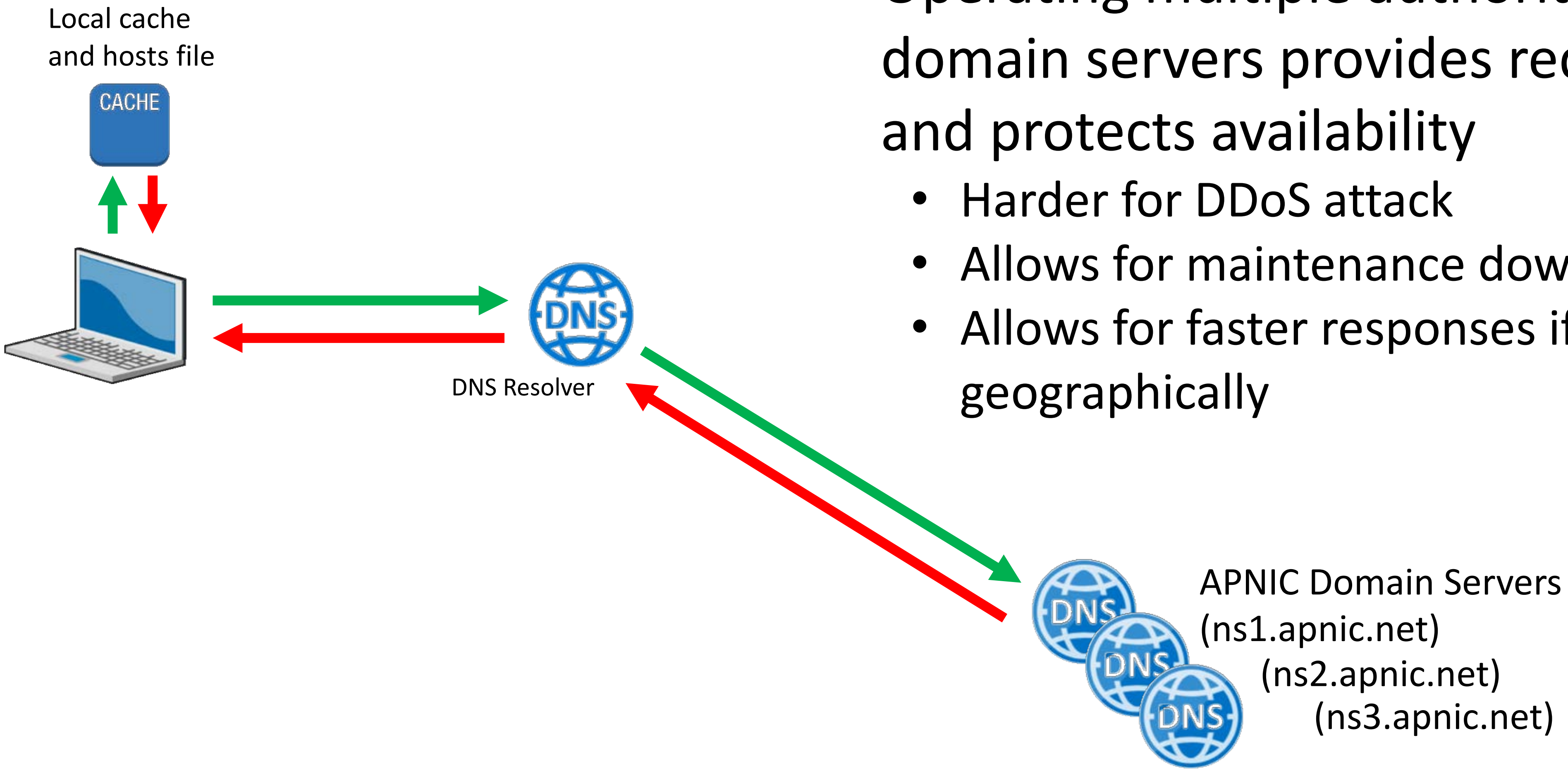
- DNS over TLS and DNS over HTTPS provide encryption to protect the confidentiality of the requests and responses

Making DNS Secure - Cryptographic Hashes



- DNS Security Extensions (DNSSEC) provides integrity checking, ensuring:
  - the responses are coming from the true authoritative domain server
  - that it hasn't been modified along the way
- Doesn't provide any protection of confidentiality

Making DNS Secure - Redundancy



- Operating multiple authoritative domain servers provides redundancy and protects availability
  - Harder for DDoS attack
  - Allows for maintenance downtime
  - Allows for faster responses if spread geographically

Making DNS Secure - Endpoints

- Don’t forget the basics!
  - Endpoint protection including anti-virus/anti-malware
  - Users not running with administrator privileges
  - Updating operating systems and applications

- There’s also some different DNS protection techniques for endpoints and even IoT devices
  - Configure your own DNS RPZ (Response Policy Zones)
    - This lets you block whatever you like
  - Use a public RPZ such as Quad9.net (set DNS = 9.9.9.9)
    - Quad9 only blocks malicious domains

Conclusion

- Domain names and DNS are more complex than most people think
- With complexity comes risk
- Make sure to identify all gaps in systems and digital supply chain
- Defence in depth is important, even for low-level infrastructure