THREAT INTELLIGENCE INSIGHTS DNS-BASED DATA EXFILTRATION

TOPIC

1. DNS
2. DNS Exfiltration
3. Deep in Death
4. Detection System

Part 1 -DNS

Topic – Part 1 - DNS

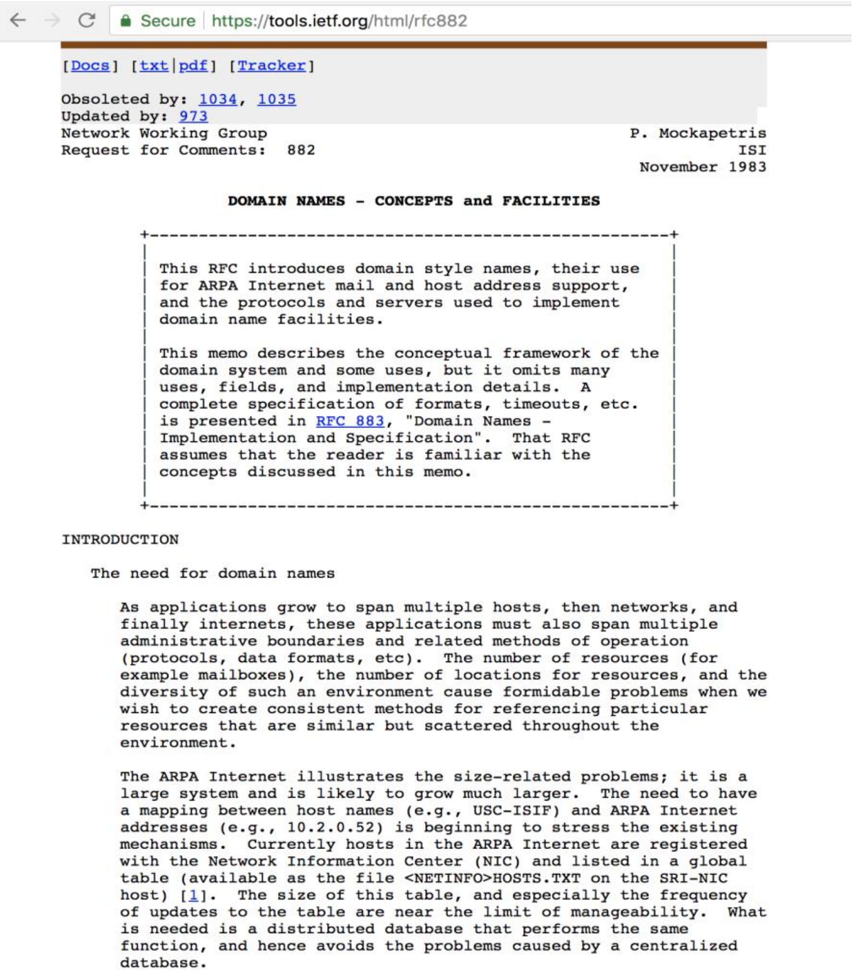
1. A Brief Background
2. RFC882
3. Root Servers
4. DNS Struct, DNS Message,
5. DNS Query, DNS Response
6. Domain Name in Message Format

DNS – A Brief Background

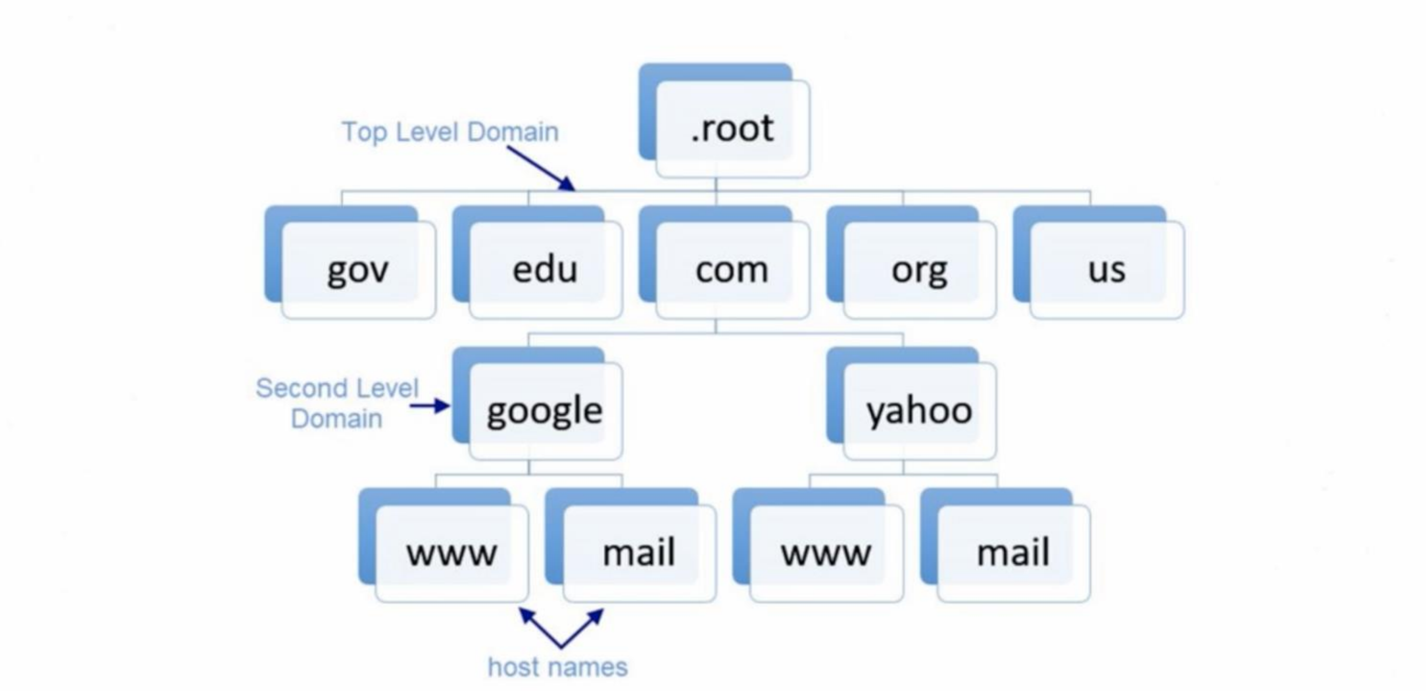
DNS Protocol

- DNS is mainly designed to resolve a hostname query to an ip address response
- The query is performed recursively, starting from the root DNS name servers until reaching the authoritative name server defined for queried domain.

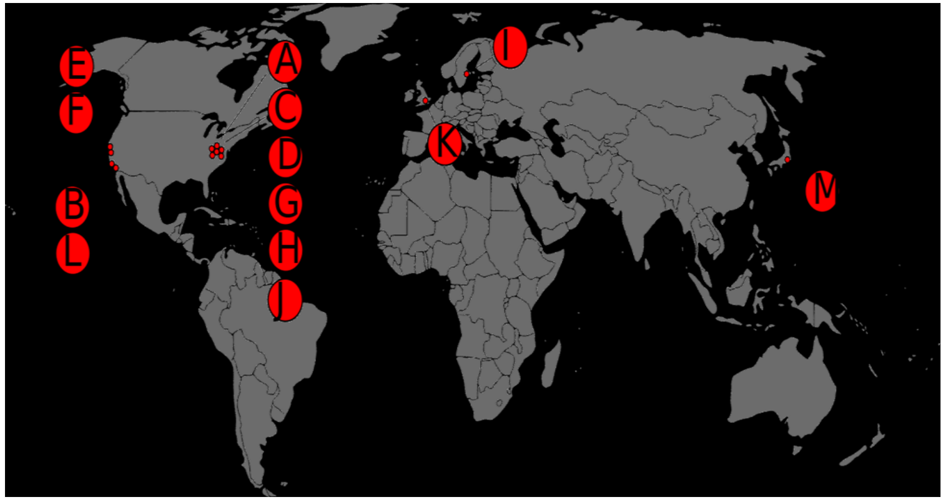
RFC 882 - November 1983

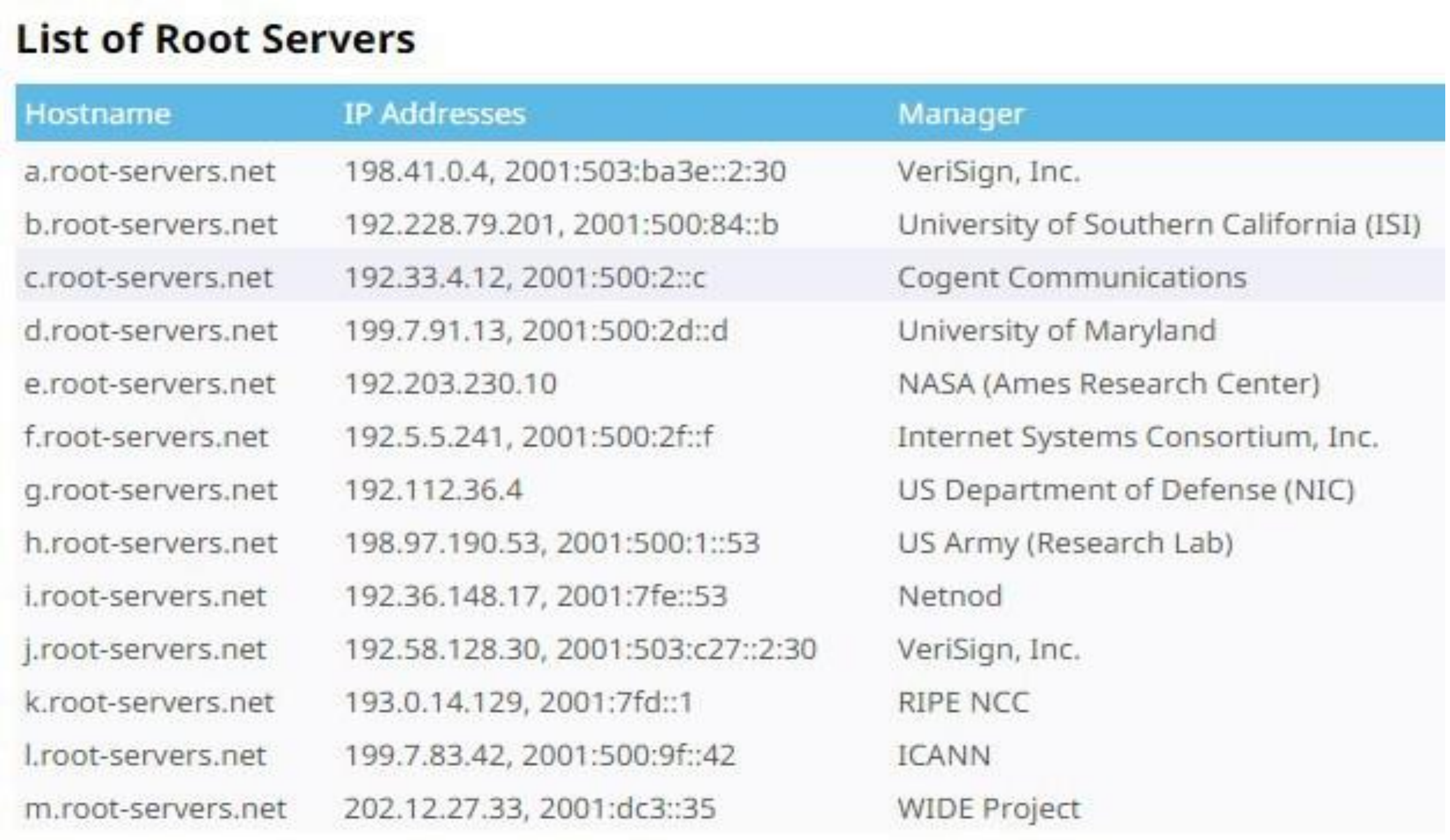


```
[Docs] [txt|pdf] [Tracker]

Obsoleted by: 1034, 1035
Updated by: 973
Network Working Group                                    P. Mockapetris
Request for Comments:  882                                          ISI
                                                          November 1983

                 DOMAIN NAMES - CONCEPTS and FACILITIES

        +-----------------------------------------------------+
        |                                                     |
        | This RFC introduces domain style names, their use   |
        | for ARPA Internet mail and host address support,    |
        | and the protocols and servers used to implement     |
        | domain name facilities.                             |
        |                                                     |
        | This memo describes the conceptual framework of the |
        | domain system and some uses, but it omits many      |
        | uses, fields, and implementation details.  A        |
        | complete specification of formats, timeouts, etc.   |
        | is presented in RFC 883, "Domain Names -            |
        | Implementation and Specification".  That RFC        |
        | assumes that the reader is familiar with the        |
        | concepts discussed in this memo.                    |
        |                                                     |
        +-----------------------------------------------------+

INTRODUCTION

   The need for domain names

      As applications grow to span multiple hosts, then networks, and
      finally internets, these applications must also span multiple
      administrative boundaries and related methods of operation
      (protocols, data formats, etc).  The number of resources (for
      example mailboxes), the number of locations for resources, and the
      diversity of such an environment cause formidable problems when we
      wish to create consistent methods for referencing particular
      resources that are similar but scattered throughout the
      environment.

      The ARPA Internet illustrates the size-related problems; it is a
      large system and is likely to grow much larger.  The need to have
      a mapping between host names (e.g., USC-ISIF) and ARPA Internet
      addresses (e.g., 10.2.0.52) is beginning to stress the existing
      mechanisms.  Currently hosts in the ARPA Internet are registered
      with the Network Information Center (NIC) and listed in a global
      table (available as the file <NETINFO>HOSTS.TXT on the SRI-NIC
      host) [1].  The size of this table, and especially the frequency
      of updates to the table are near the limit of manageability.  What
      is needed is a distributed database that performs the same
      function, and hence avoids the problems caused by a centralized
      database.
```



Root Servers

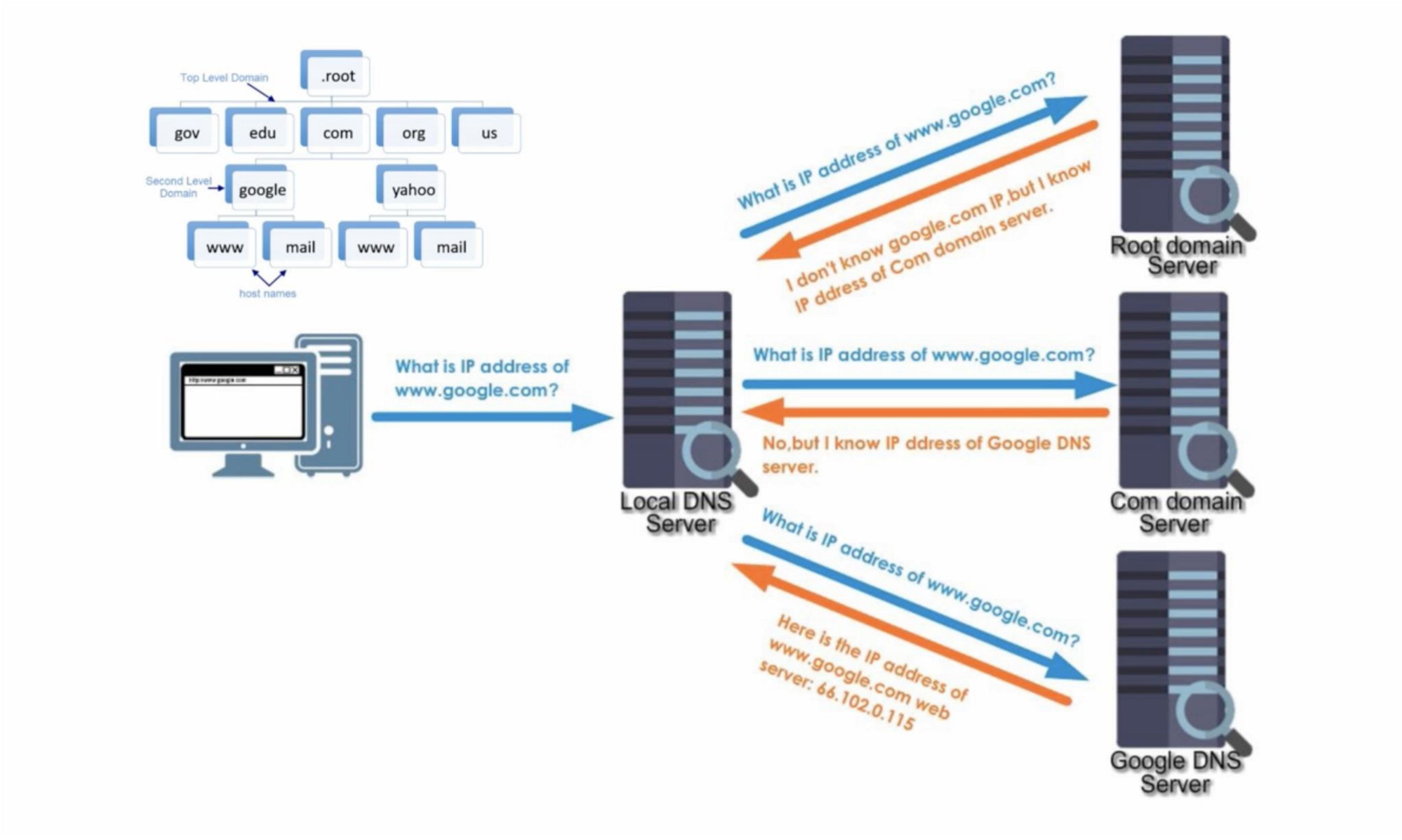




List of Root Servers

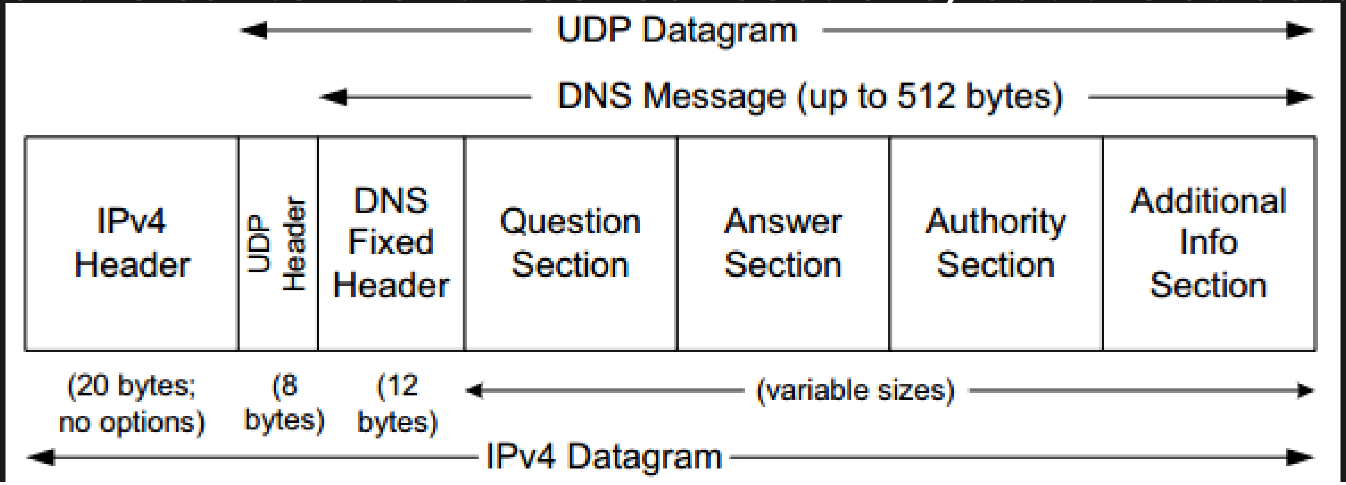
Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

DNS Struct

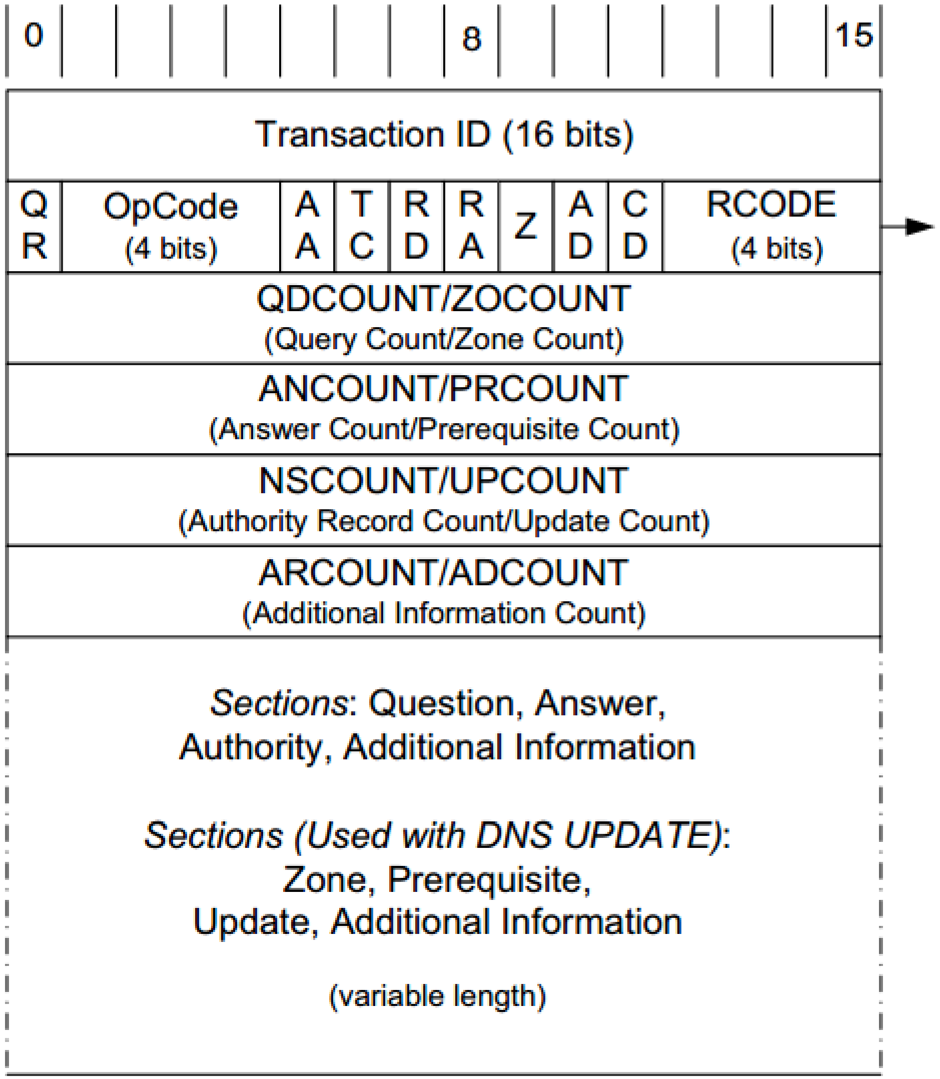

.root
Top Level Domain
gov
edu
com
org
us
Second Level Domain
google
yahoo
www
mail
www
mail
host names
What is IP address of www.google.com?
Local DNS Server
What is IP address of www.google.com?
I don't know google.com IP,but I know IP ddress of Com domain server.
Root domain Server
What is IP address of www.google.com?
No,but I know IP ddress of Google DNS server.
Com domain Server
What is IP address of www.google.com?
Here is the IP address of www.google.com web server: 66.102.0.115
Google DNS Server

DNS Messages 1/2

- There are two types of DNS messages, queries And replies, they both have the same format.
- Each message consists of a header and four sections: question, answer, authority, additional
- The header field “flags” control the content of these four sections, but the structure of all DNS messages is the same.



DNS Messages 2/2



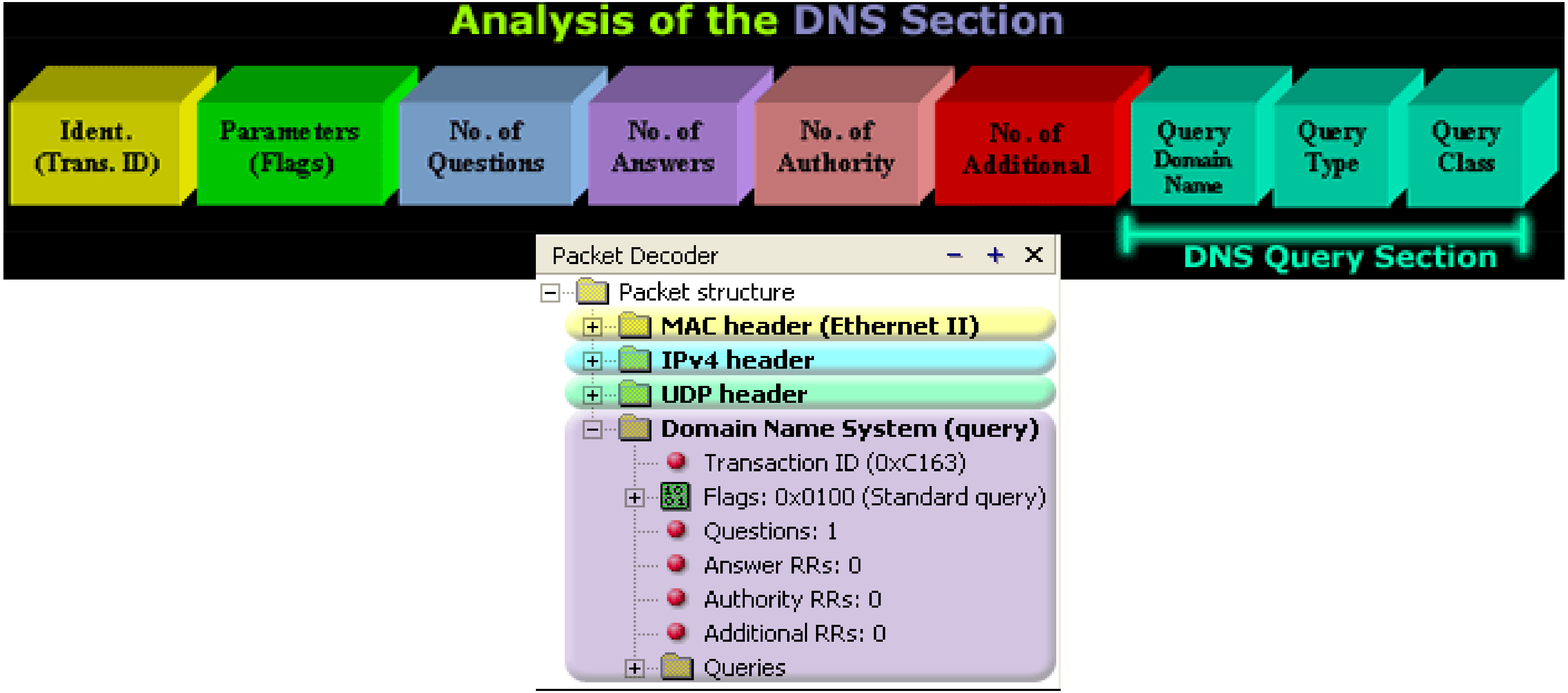
0
8
15
Transaction ID (16 bits)
QR
OpCode (4 bits)
AA
TC
RD
RA
Z
AD
CD
RCODE (4 bits)
QDCOUNT/ZOCOUNT (Query Count/Zone Count)
ANCOUNT/PRCOUNT (Answer Count/Prerequisite Count)
NSCOUNT/UPCOUNT (Authority Record Count/Update Count)
ARCOUNT/ADCOUNT (Additional Information Count)
Sections: Question, Answer, Authority, Additional Information
Sections (Used with DNS UPDATE): Zone, Prerequisite, Update, Additional Information
(variable length)

Flags:
QR: Query(0)/Response(1)
AA: Authoritative Answer
TC: Truncated Answer
RD: Recursion Desired
RA: Recursion Available
Z: Zero
AD: Authentic Data [RFC4035]
CD: Checking Disabled [RFC4035]

OpCodes (common values):
Query (0) – Regular Query
Notify (4) – DNS NOTIFY [RFC1996]
Update (5) – DNS UPDATE [RFC2136]

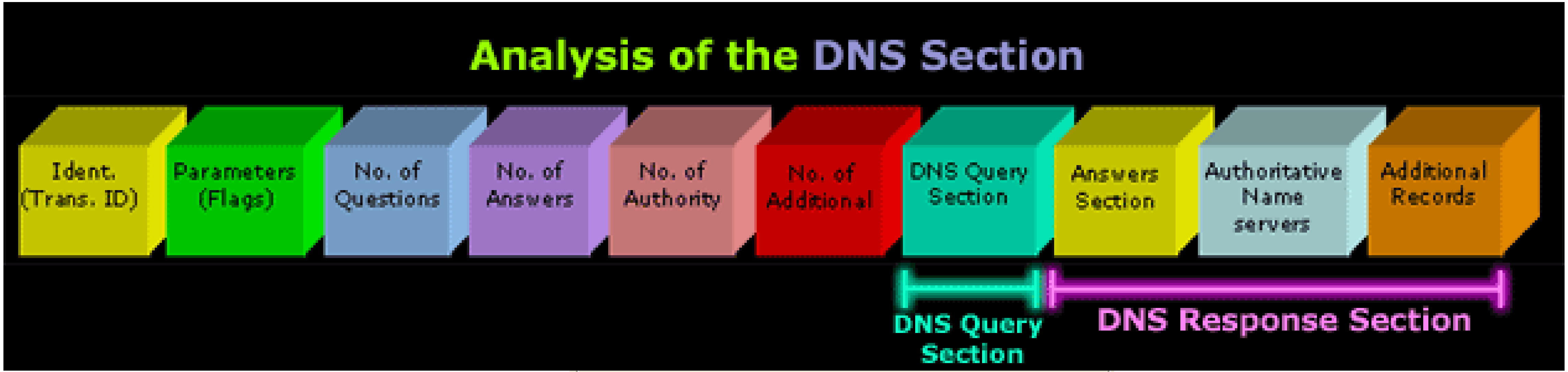
RCODEs (common values):
NoError (0) – No Error
FormErr (1) – Format Error
ServFail (2) – Server Failure
NXDomain (3) – Non-existent Domain
NotImp (4) – Not Implemented
Refused (5) – Query Refused

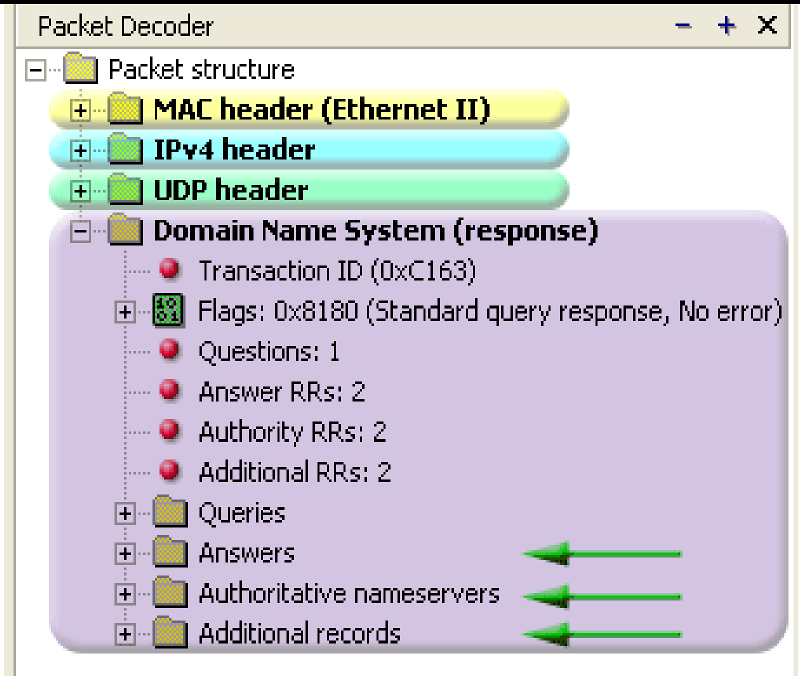
DNS Query



- Packet structure
  - MAC header (Ethernet II)
  - IPv4 header
  - UDP header
  - Domain Name System (query)
    - Transaction ID (0xC163)
    - Flags: 0x0100 (Standard query)
    - Questions: 1
    - Answer RRs: 0
    - Authority RRs: 0
    - Additional RRs: 0
    - Queries

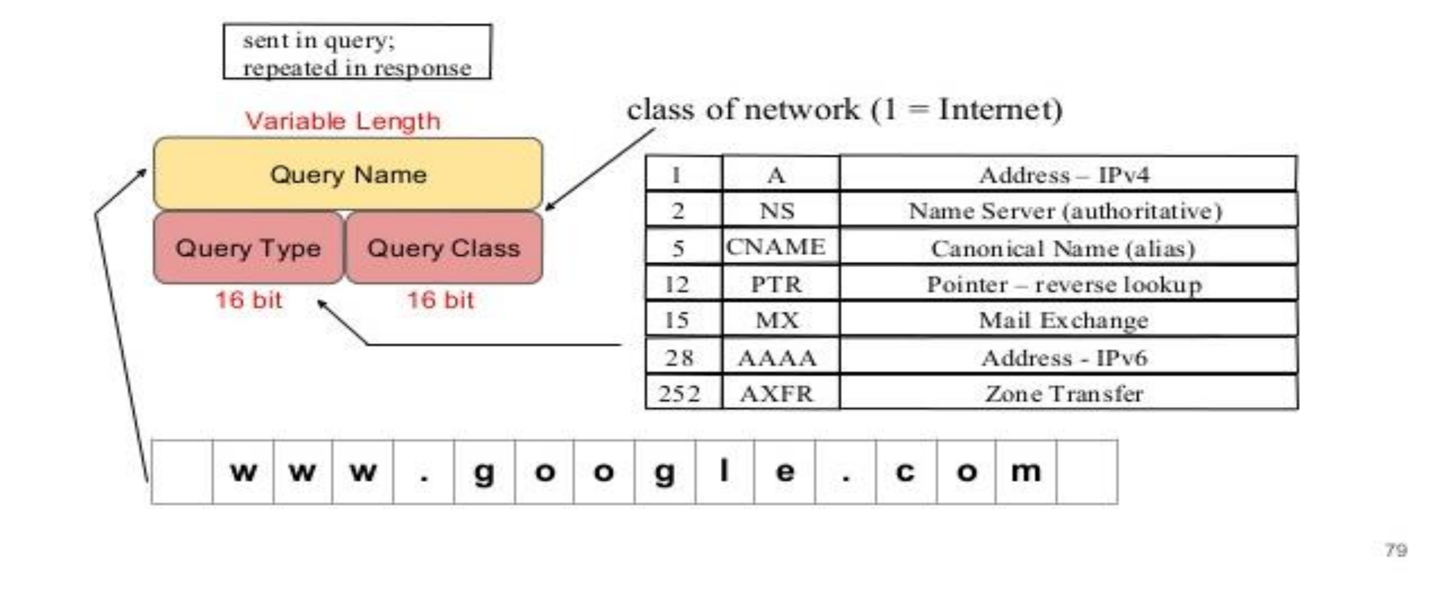
DNS Response



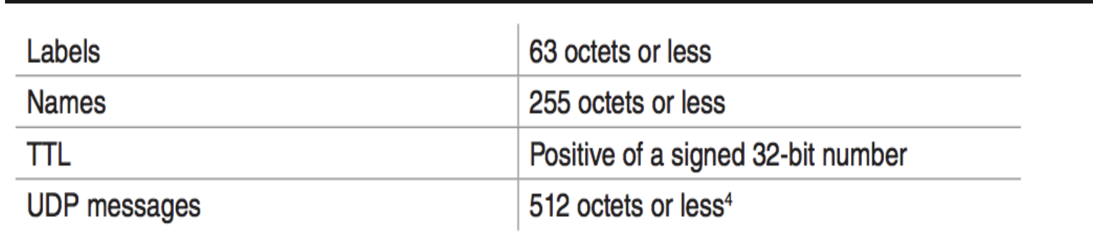


- Packet structure
  - MAC header (Ethernet II)
  - IPv4 header
  - UDP header
  - Domain Name System (response)
    - Transaction ID (0xC163)
    - Flags: 0x8180 (Standard query response, No error)
    - Questions: 1
    - Answer RRs: 2
    - Authority RRs: 2
    - Additional RRs: 2
    - Queries
    - Answers
    - Authoritative nameservers
    - Additional records

Domain Name in Message Format



1	A	Address – IPv4
2	NS	Name Server (authoritative)
5	CNAME	Canonical Name (alias)
12	PTR	Pointer – reverse lookup
15	MX	Mail Exchange
28	AAAA	Address - IPv6
252	AXFR	Zone Transfer



Labels	63 octets or less
Names	255 octets or less
TTL	Positive of a signed 32-bit number
UDP messages	512 octets or less[4]

- Various objects and parameters in the DNS have size limits. The size limits are listed below. Some can be easily changed, while others are more fundamental

Part 2 -DNS Exfiltration

Topic – Part 2 - DNS Exfiltration

1. Why is DNS a problem?
2. How does it work?
3. Attacker’s Motivation
4. Threat Landscape
5. DNS Tunneling VS DNS Exfiltration Malware

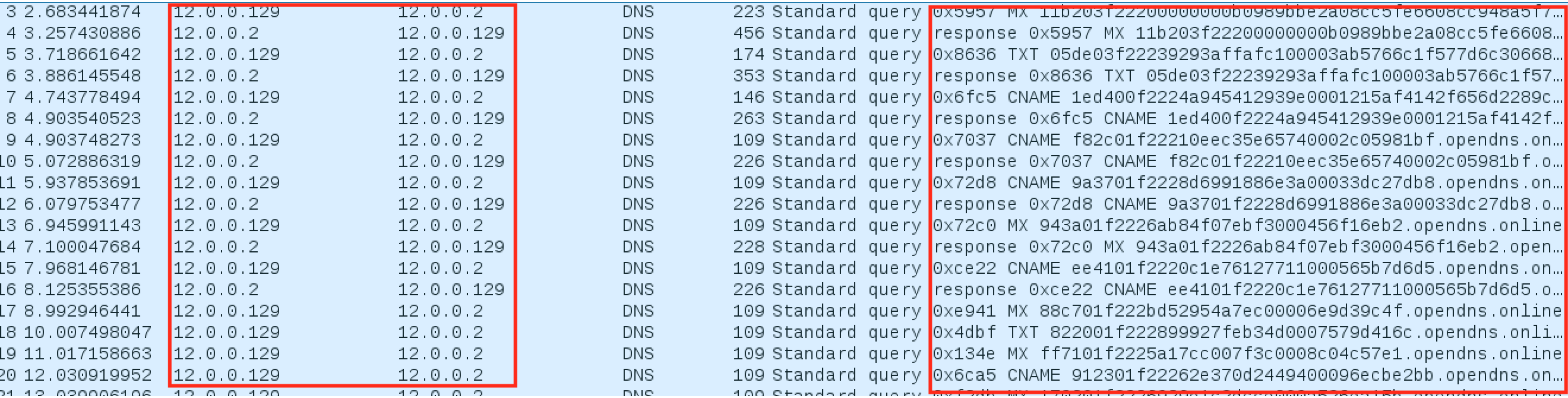
Why is DNS a problem?

Must be allowed through firewall

Cannot block port 53 (DNS)

Most environments don’t monitor DNS requests

DNS Exfiltration



```
 3 2.683441874  12.0.0.129     12.0.0.2      DNS   223 Standard query 0x5957 MX 11b203f22200000000b0989bbe2a08cc5fe6608cc948a5f7…
 4 3.257430886  12.0.0.2       12.0.0.129    DNS   456 Standard query response 0x5957 MX 11b203f22200000000b0989bbe2a08cc5fe6608…
 5 3.718661642  12.0.0.129     12.0.0.2      DNS   174 Standard query 0x8636 TXT 05de03f22239293affafc100003ab5766c1f577d6c30668…
 6 3.886145548  12.0.0.2       12.0.0.129    DNS   353 Standard query response 0x8636 TXT 05de03f22239293affafc100003ab5766c1f57…
 7 4.743778494  12.0.0.129     12.0.0.2      DNS   146 Standard query 0x6fc5 CNAME 1ed400f2224a945412939e0001215af4142f656d2289c…
 8 4.903540523  12.0.0.2       12.0.0.129    DNS   263 Standard query response 0x6fc5 CNAME 1ed400f2224a945412939e0001215af4142f…
 9 4.903748273  12.0.0.129     12.0.0.2      DNS   109 Standard query 0x7037 CNAME f82c01f22210eec35e65740002c05981bf.opendns.on…
10 5.072886319  12.0.0.2       12.0.0.129    DNS   226 Standard query response 0x7037 CNAME f82c01f22210eec35e65740002c05981bf.o…
11 5.937853691  12.0.0.129     12.0.0.2      DNS   109 Standard query 0x72d8 CNAME 9a3701f2228d6991886e3a00033dc27db8.opendns.on…
12 6.079753477  12.0.0.2       12.0.0.129    DNS   226 Standard query response 0x72d8 CNAME 9a3701f2228d6991886e3a00033dc27db8.o…
13 6.945991143  12.0.0.129     12.0.0.2      DNS   109 Standard query 0x72c0 MX 943a01f2226ab84f07ebf3000456f16eb2.opendns.online
14 7.100047684  12.0.0.2       12.0.0.129    DNS   228 Standard query response 0x72c0 MX 943a01f2226ab84f07ebf3000456f16eb2.open…
15 7.968146781  12.0.0.129     12.0.0.2      DNS   109 Standard query 0xce22 CNAME ee4101f2220c1e76127711000565b7d6d5.opendns.on…
16 8.125355386  12.0.0.2       12.0.0.129    DNS   226 Standard query response 0xce22 CNAME ee4101f2220c1e76127711000565b7d6d5.o…
17 8.992946441  12.0.0.129     12.0.0.2      DNS   109 Standard query 0xe941 MX 88c701f222bd52954a7ec00006e9d39c4f.opendns.online
18 10.007498047 12.0.0.129     12.0.0.2      DNS   109 Standard query 0x4dbf TXT 822001f222899927feb34d0007579d416c.opendns.onli…
19 11.017158663 12.0.0.129     12.0.0.2      DNS   109 Standard query 0x134e MX ff7101f2225a17cc007f3c0008c04c57e1.opendns.online
20 12.030919952 12.0.0.129     12.0.0.2      DNS   109 Standard query 0x6ca5 CNAME 912301f22262e370d2449400096ecbe2bb.opendns.on…
```

DNS Exfiltration – How Does it work?

DNS Data Exfiltration

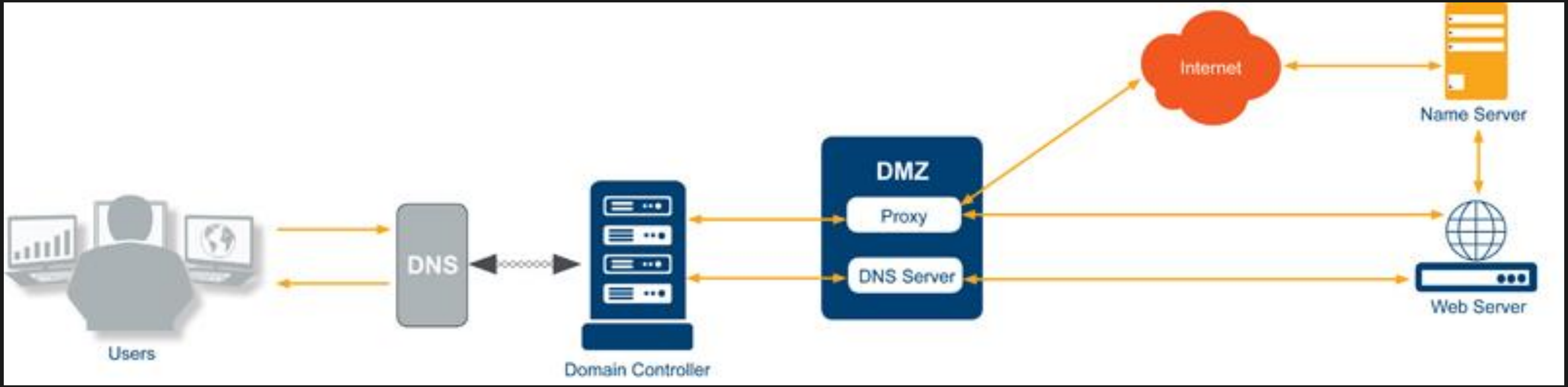
- An attacker first sets-up his own authoritative name server
- Any compromised machine that queries that name server is a defacto established communication channel between the machine and the name server.
- Extermely easy and cheap

DNS Exfiltration – Attacker’s Motivation

- DNS is not an ideal covert channel:
  - Limited query size (up to 255 bytes)
  - Unreliable (order of message is not guaranteed)
- However, DNS is:
  - A cornerstone of the Internet; available in almost every network
  - Rarely monitored compared to HTTP,FTP and e-mail protocols

DNS Exfiltration – Threat Landscape

- DNS Tunneling Software
- DNS Exfiltration Malware



DNS Exfiltration – Threat Landscape

DNS Tunneling Software

- Common Usage
  - Web browsing over the DNS
  - Remote desktop protocols
- Examples:
  - OzymanDNS-Tunneling SSH over DNS
  - Iodine
  - DNSCat
  - Dns2tcp

DNS Exfiltration Malware

- Common usage
  - Sensitivities data thief (e.g., passwords)
  - Command and control channel
- Examples:
  - FrameworkPOS(2014)
  - BernhardPOS(2015)
  - Win32.Backdoor.Denis(2017)

Part 3 - deep in death

Topic - Part 3 - DEEP IN DEATH

1. What is DNS Tunneling?
2. Communication Patterns
3. What is this Shellcode ?
4. Is all shellcode created equal ?
5. So how does it work ?
6. Staged Loading shellcode ?
7. Down And Dirty In Detail !
8. You think you’re better than us ?!
9. DNS Tunneling Countermeasures…

What is DNS Tunneling?

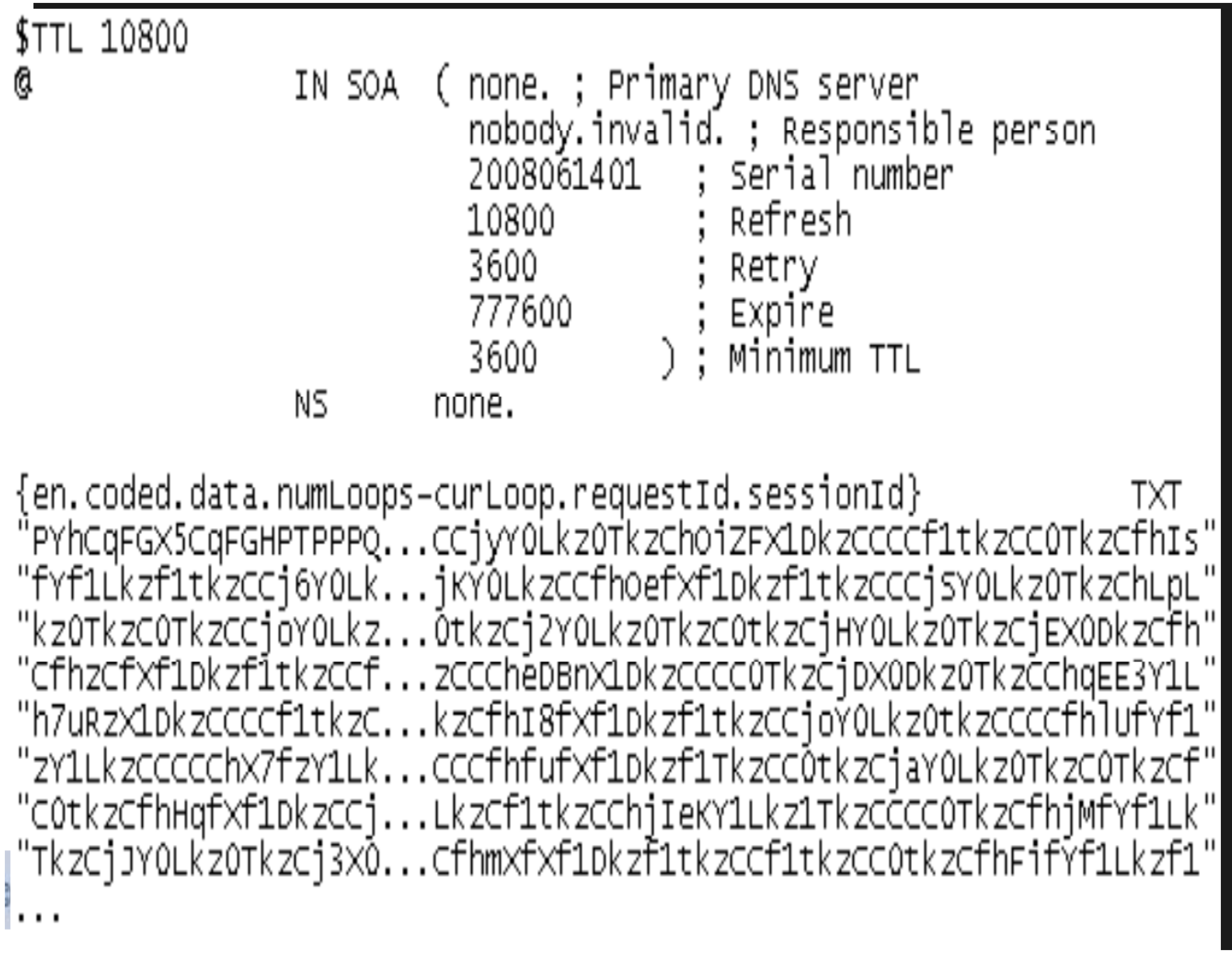
DNS Tunneling Restrictions

- Request
  - Maximum of 253 characters in domain
  - Maximum of 63 characters per subdomain
  - Case-insensitive (so we use Base32 encoding)
  - TXT request to get maximum characters in response
    - the limit to a TXT string is 255
    - the limit to a UDP packet is 512
    - the limit to total of TXT data for a given record is 65535
- DNS Tunneling Shellcode Request Format:
  - en.coded.data.numloops-curloop.requestid.sessionid.domainname.com

DNS Exfiltration – Communication Patterns

DNS Tunneling Restrictions

- TXT Response
  - Can hold large amounts of data (Great for Tunneling)
  - Case-insensitive (p g) We use Al phanumeric Shellcode encoding)
- DNS Tunneling Shellcode DNS TXT Response Format:



```
$TTL 10800
@               IN SOA  ( none. ; Primary DNS server
                          nobody.invalid. ; Responsible person
                          2008061401    ; Serial number
                          10800         ; Refresh
                          3600          ; Retry
                          777600        ; Expire
                          3600        ) ; Minimum TTL
                NS      none.

{en.coded.data.numLoops-curLoop.requestId.sessionId}            TXT
"PYhCqFGX5CqFGHPTPPPQ...CCjyY0Lkz0TkzChoiZFX1DkzCCCCf1tkzCC0TkzCfhIs"
"fYf1Lkzf1tkzCCj6Y0Lk...jKY0LkzCCfhoefXf1Dkzf1tkzCCCjSY0Lkz0TkzChLpL"
"kz0TkzC0TkzCCjoY0Lkz...0tkzCj2Y0Lkz0TkzC0tkzCjHY0Lkz0TkzCjEX0DkzCfh"
"CfhzCfXf1Dkzf1tkzCCf...zCCCheDBnX1DkzCCCCC0TkzCjDX0Dkz0TkzCChqEE3Y1L"
"h7uRzX1DkzCCCCf1tkzC...kzCfhI8fXf1Dkzf1tkzCCjoY0Lkz0tkzCCCCfhlufYf1"
"zY1LkzCCCCChX7fzY1Lk...CCCfhfufXf1Dkzf1TkzCC0tkzCjaY0Lkz0TkzC0TkzCf"
"C0tkzCfhHqfXf1DkzCCj...LkzCf1tkzCChjIeKY1Lkz1TkzCCCC0TkzCfhjMfYf1Lk"
"TkzCjJY0Lkz0TkzCj3X0...CfhmXfXf1Dkzf1tkzCCf1tkzCC0tkzCfhFifYf1Lkzf1"
...
```

Part 4 – Detection System

Topic - Part 4 - Detection System

1. Detection Goals
2. Communication Patterns
3. Detection/Mitigation
4. Endpoint vs Network Solutions
5. Key Consideration for Any Detection System

DNS Exfiltration - Midway

- The next part deals with detection of DNS tunneling and malware
- But first, what did we establish so far about DNS exfiltration?
  - Millions of credit cards stolen thus far
  - Popular attack due to an easy attacker setup and lesser security enforcement
  - Can be divided to two classes: DNS tunneling software and malware.
  - Capturing both is a challenge due to their different communication patterns

DNS Exfiltration – Detection Goals

- Any Seure system should detect both:
  - DNS tunneling software
  - DNS exfiltratin malware
- Isn’t the detection of both classes practically the same?
  - No, The communication patterns of both classes are significantly different.

DNS Exfiltration – Communication Patterns

DNS Tunneling Software

- Reliable
  - Frequent keep-alive messages
- Bi-directional and interactive
  - “Lengthy” responses
- Verbose
  - RDP / Web browsing with 255 byte messages requires a large number of messages

DNS Exfiltration Malware

- “Opportunistic” querying
  - A single credit card per swipe
- Possibly unidirectional
  - ACK response or no response
- Mostly unexpected
  - New attackers improve the ability to go ”under the radar”

Endpoint vs. Network Solutions

Endpoints Solutions

- Can leverage user context (running processes)

Network Solutions

- Can leverage global visibility (large scale bots, striking out widely used services)
- Platform independent
- Ease of integration

Key Considerations for Any Detection System

- Where does the solution resides?
    - Endpoint vs. Network Solutions Comparison
- What is the expected result?
    - Analysis Tool vs. Automatic Blocking
- How effective is the solution against new malware threats?
    - Manually Chosen Rules vs. Machine Learning
    - Actionable Reporting