Cloud Malware Distribution

DNS will be your friend

IX Foro de Seguridad RedIRIS

RedIRIS

Francisco J. Gómez Rodríguez (ffranz@iniqua.com):

- Computer engineering (EUI-UPM)
- Security research (Telefonica R&D)
- **dig ffranz.cmdns.h4ck.me TXT**

Carlos Díaz Hidalgo (charlie@tid.es):

- Telecommunications Engineer (ETSITM-UPM)
- GPEN, GCIH, OPST, ITILF and CCNA.
- Technology Specialist in Ethical Hacking (Telefonica R&D)
- **dig charlie.cmdns.h4ck.me TXT**

- 01 Introduction
- 02 DNS in a nutshell
- 03 Our history
  - Implementation
  - Improvement
- 04 Real world
- 05 Results

- 01 Introduction
- 02 DNS in a nutshell
- 03 Our history
  - Implementation
  - Improvement
- 04 Real world
- 05 Results

01 Malware on legitimate DNS

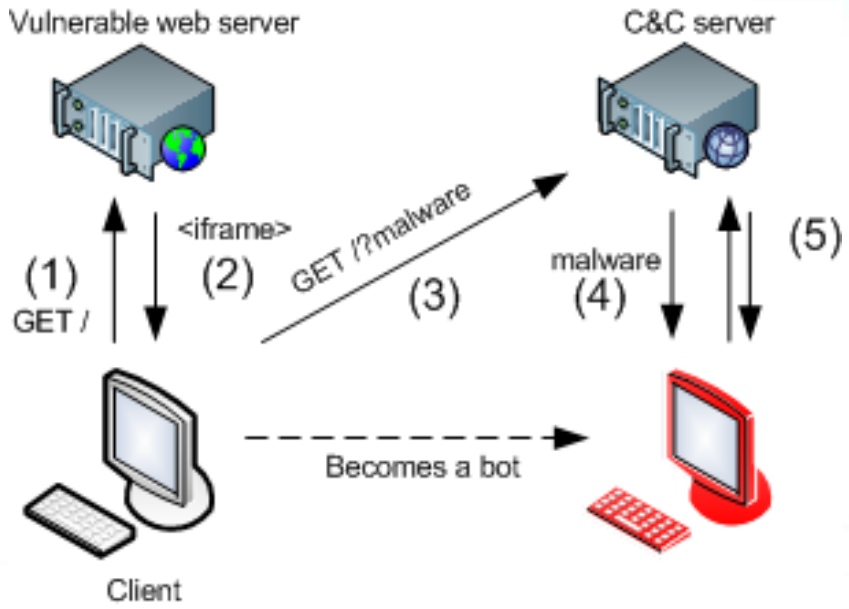
- Nowadays, many legitimate Web sites are serving malware.
  - But … Attacker must compromise the server first.
- Why couldn't we do it differently?
  - Using legitimate DNS caches.
  - We can inject malware into caches without needing to compromise them.

01 Introduction

- Cloud Malware Distribution (CMD)
  - An alternative method for malware distribution using Cache DNS services.
- Why cloud?
  - DNS service is one of the first cloud services.
- How?
  - By using the protocol and the architecture.

01

Break point (I)



Torpig

1. GET resource
2. Process resource
3. GET payload
4. Process payload
5. **Update Bot**

01 Break point (II)

abuse.ch ZeuS Tracker

megasticks.ru/au.exe

1	2011-02-23	09:55	[redacted]	DNS	Standard query A megasticks.ru
2	2011-02-23	09:55	[redacted]	DNS	Standard query A megasticks.ru
3	2011-02-23	09:55	[redacted]	DNS	Standard query response A 68.65.39.62 A 195.214.238.241 A
4	2011-02-23	09:55	[redacted]	DNS	Standard query response A 68.65.39.62 A 195.214.238.241 A
5	2011-02-23	09:55	[redacted]	TCP	mgesupervision > http [SYN] Seq=0 Win=8192 Len=0 MSS=1260
6	2011-02-23	09:55	[redacted]	TCP	http > mgesupervision [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=
7	2011-02-23	09:55	[redacted]	TCP	mgesupervision > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
8	2011-02-23	09:55	[redacted]	HTTP	GET /au.exe HTTP/1.1
9	2011-02-23	09:55	[redacted]	HTTP	[TCP Retransmission] GET /au.exe HTTP/1.1
10	2011-02-23	09:55	[redacted]	TCP	http > mgesupervision [ACK] Seq=1 Ack=436 Win=65100 Len=0
11	2011-02-23	09:55	[redacted]	TCP	[TCP segment of a reassembled PDU]
12	2011-02-23	09:55	[redacted]	TCP	[TCP segment of a reassembled PDU]

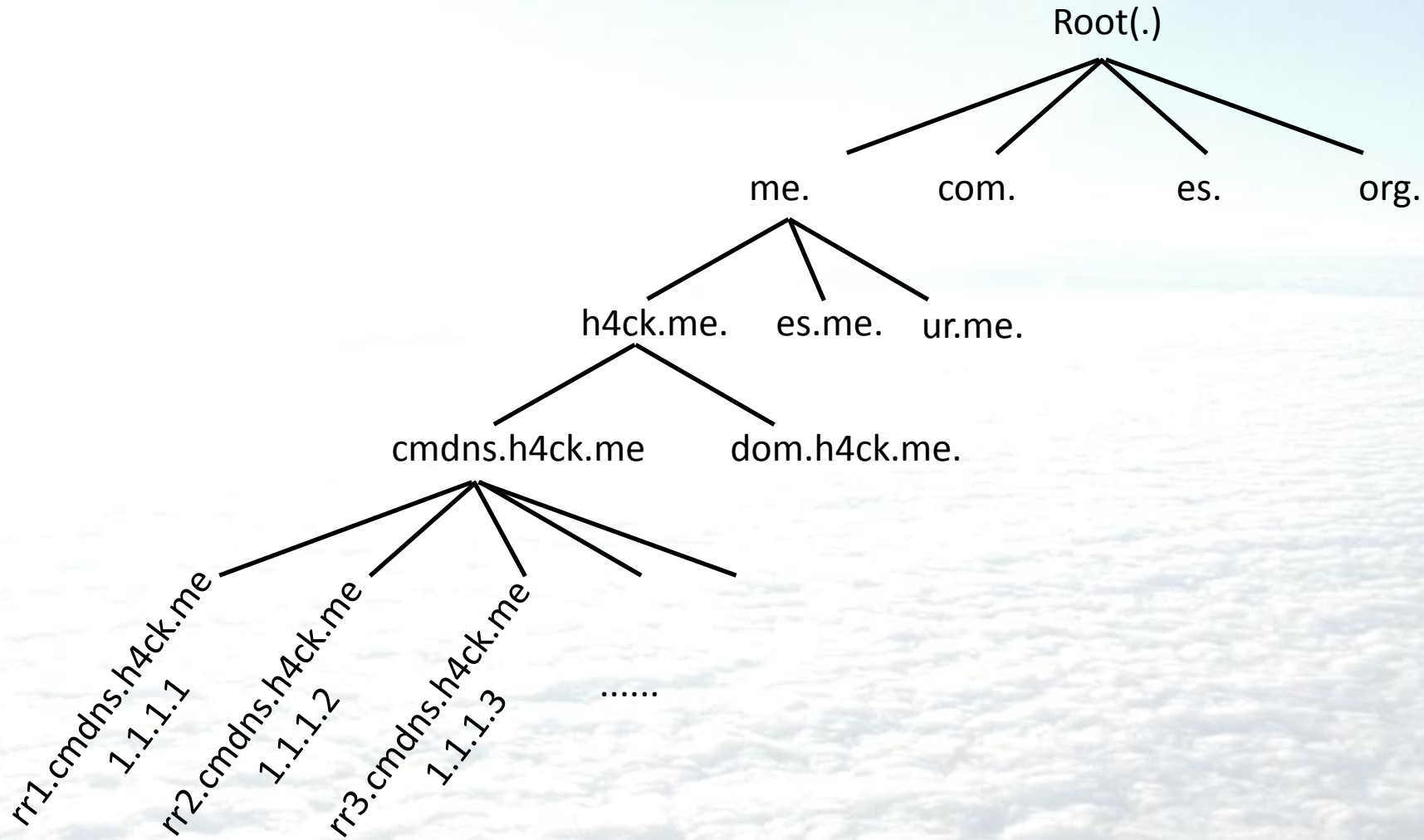
HTTP GET file

- 01 Introduction
- 02 **DNS in a nutshell**
- 03 Our history
  - Implementation
  - Improvement
- 04 Real world
- 05 Results

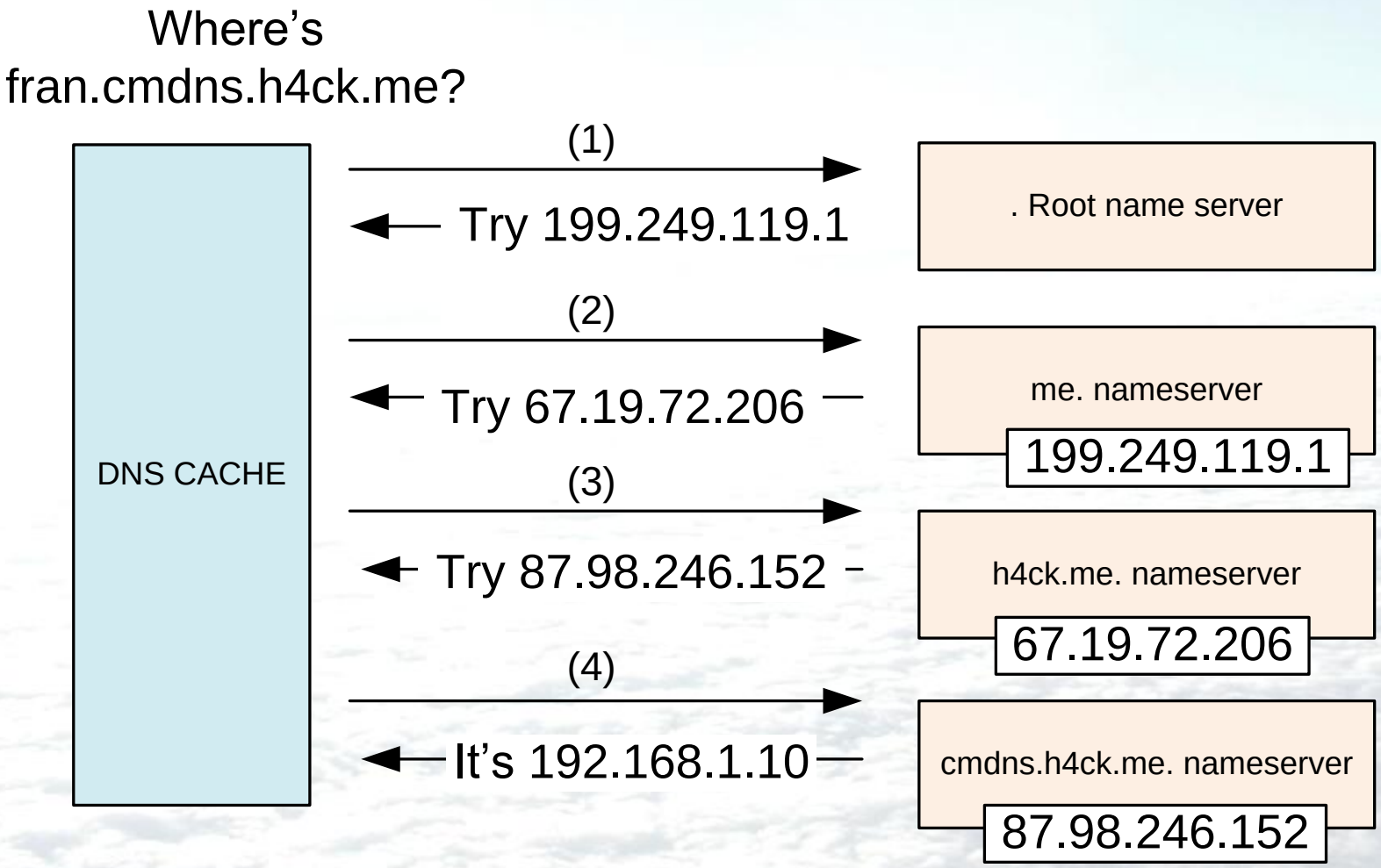
02 Architecture

- Hierarchical naming system.
- Globally deployed, universally employed.
- DNS traffic is usually allowed, even in the most restrictive environments.
- Not inspected, …, as it should be.
- **DNS is a key enabling technology for botnets.**

02 Hierarchical Architecture (I)



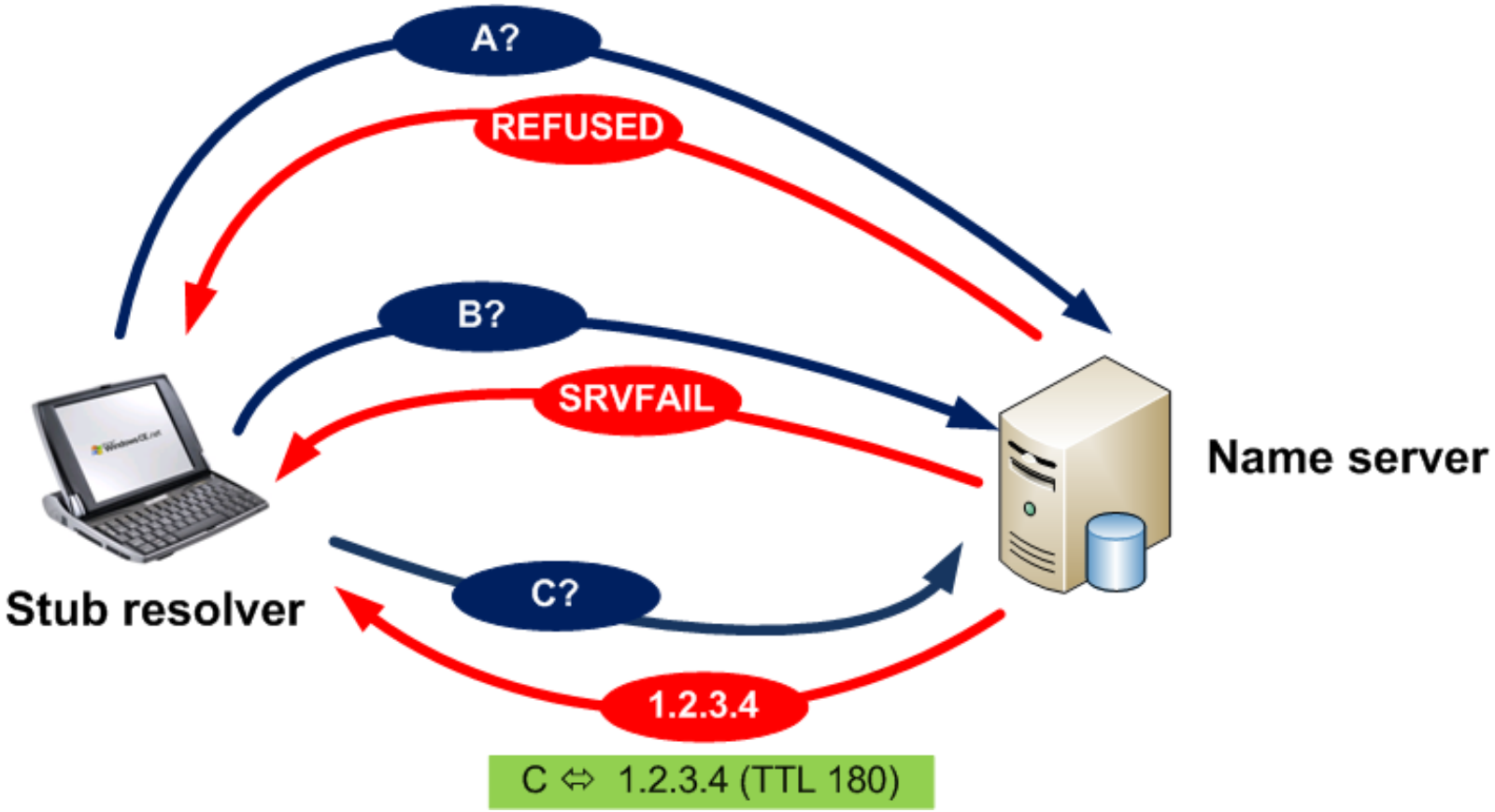
02 Hierarchical Architecture (II)



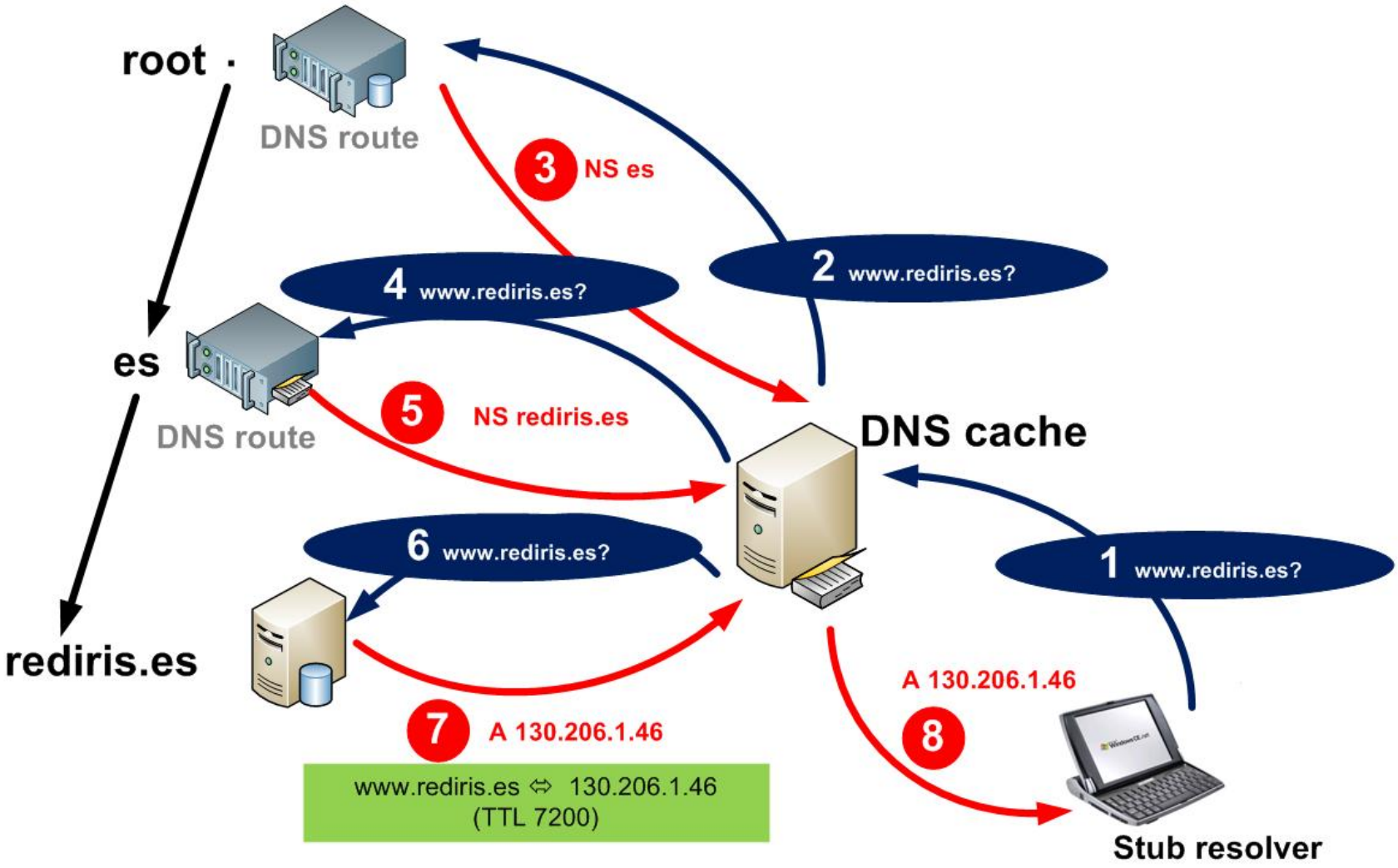
02 DNS caching

- DNS responses are cached:
  - The authoritative server uses the TTL value to set the "expiration date" for every record.
  - Other queries may reuse some parts of the lookup (quick response).
  - Negative caching is useful.
- **Although the source is gone, information remains stored.**

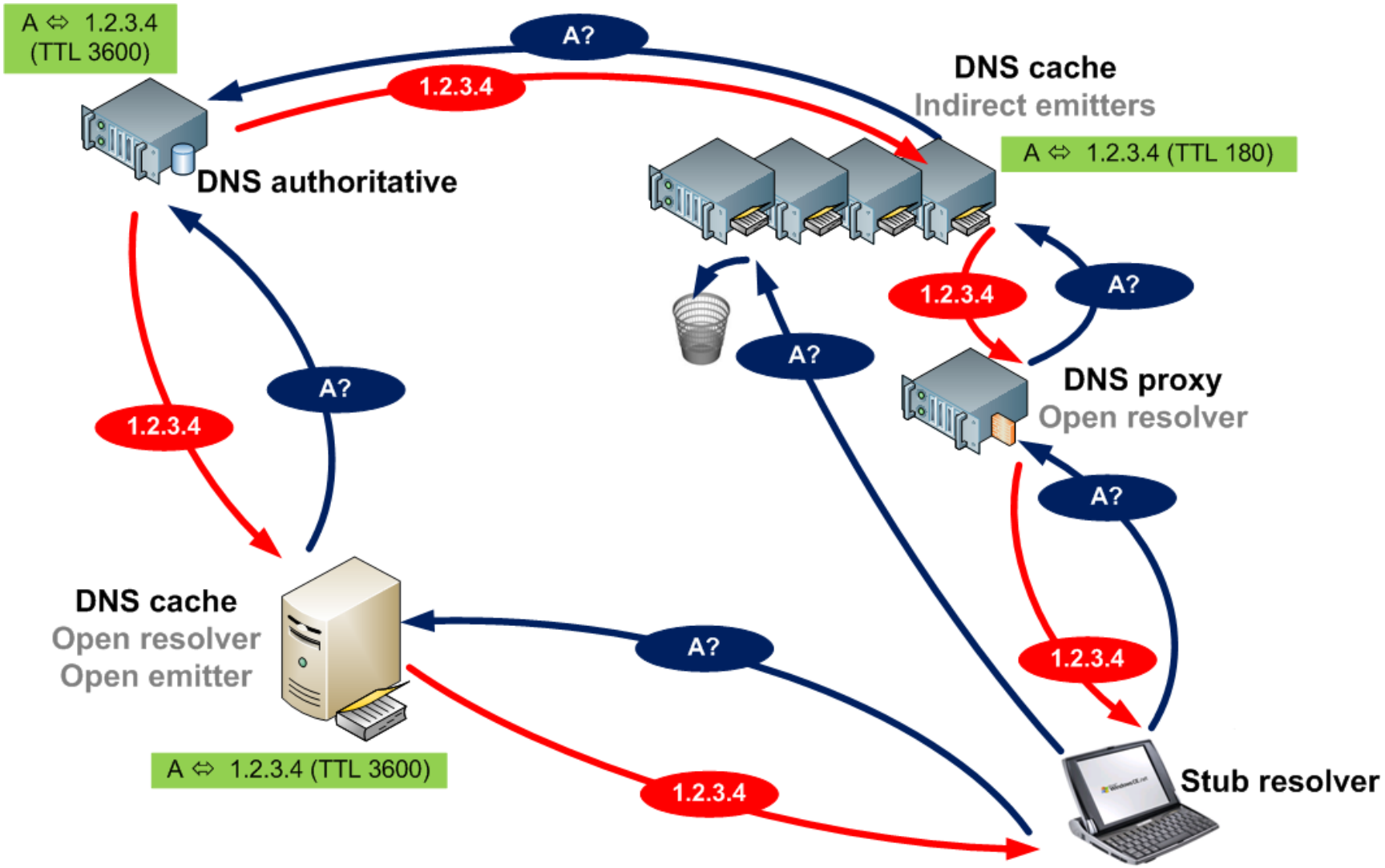
02 Types of (I)


A?
REFUSED
B?
SRVFAIL
Name server
Stub resolver
C?
1.2.3.4
C ⇔ 1.2.3.4 (TTL 180)

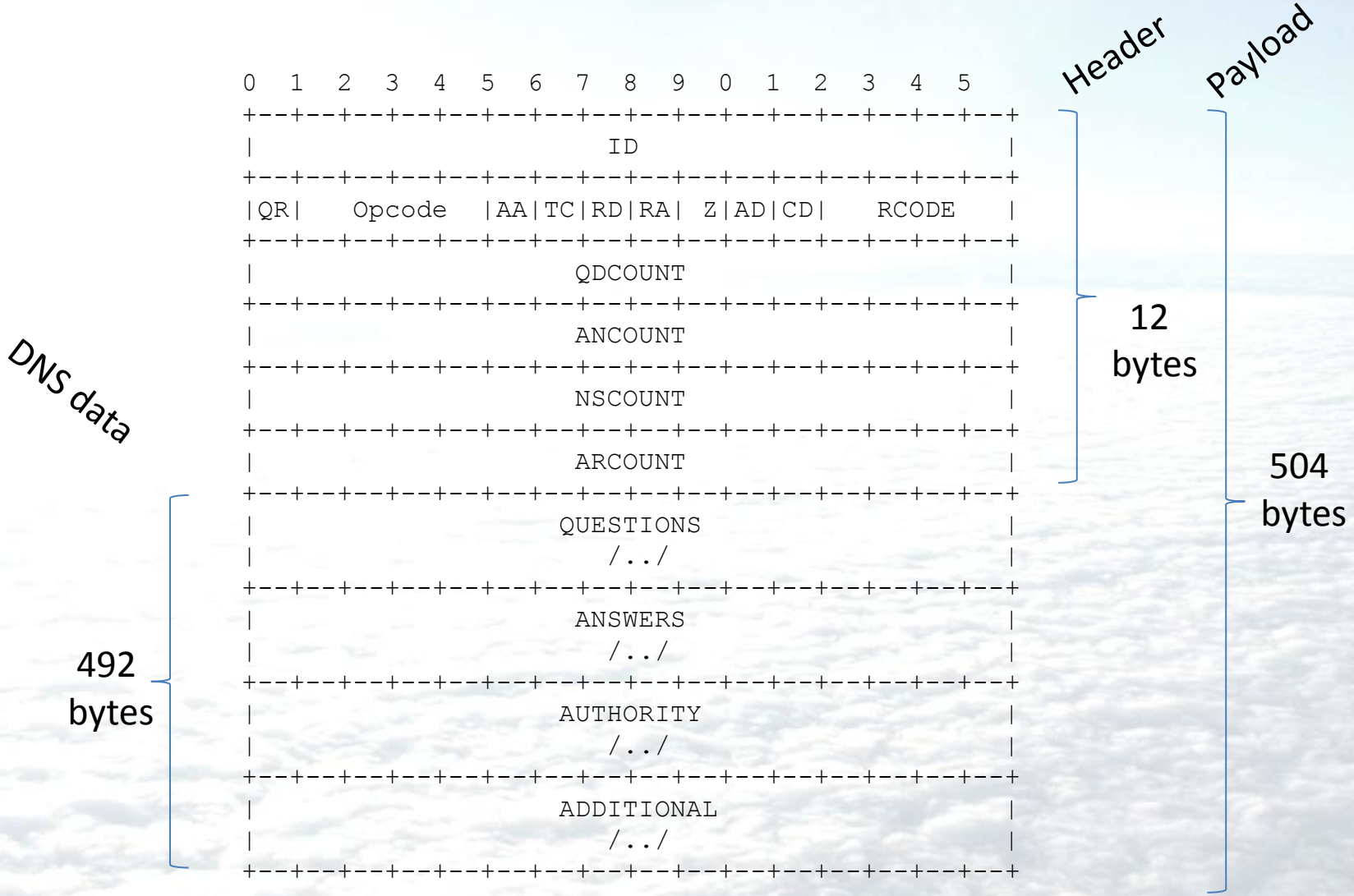
02 Types of (II)



02 Types of (III)



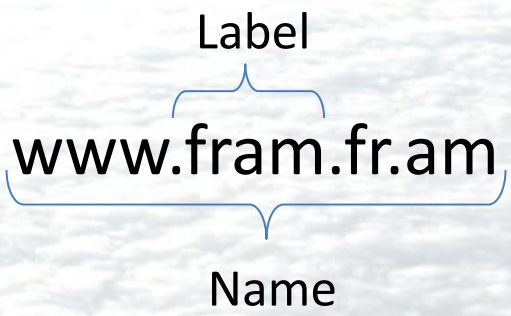
02 DNS Protocol (I)



02 DNS Protocol (II)

Resource Record Format		
Name	www.fram.fr.am	**255 octets**
Type	A	**2 octets**
Class	IN	**2 octets**
TTL	100	**4 octets**
RDLength	4	**2 octets**
RDATA	192.168.1.10	**255 octets**

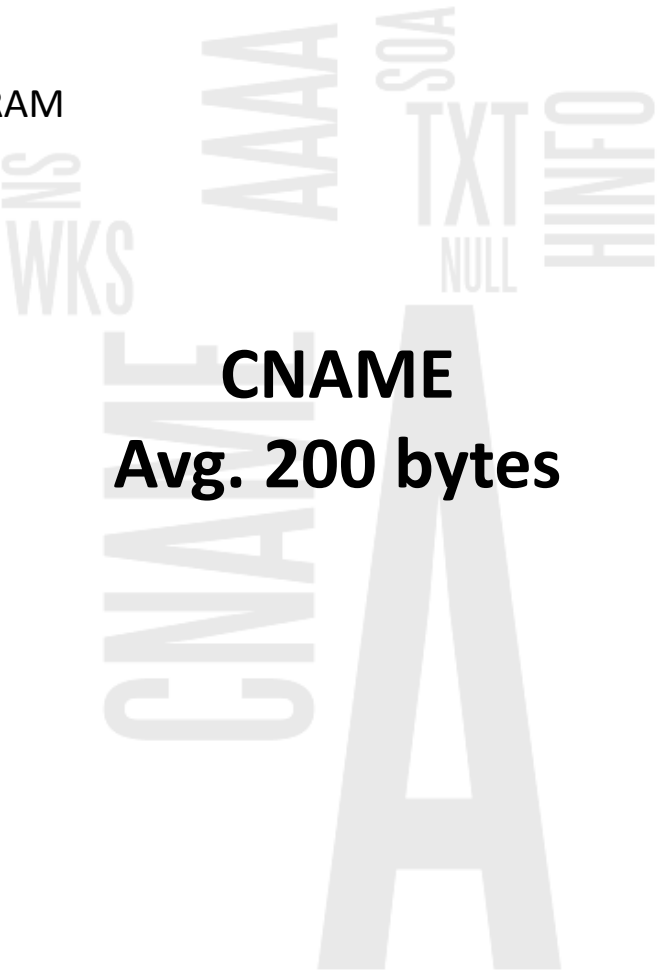
- Labels 63 octets or less
- Names 255 octets or less
- TTL 32 bit number.
- UDP msg 512 octets or less



02 DNS Protocol (III)

Types… types… types…

- A
- AAAA
- NS
- MD
- MF
- SOA
- MB
- MG
- MR
- NULL
- WKS
- PTR
- HINFO
- MINFO
- MX
- TXT
- RP
- AFSDB
- X25
- ISDN
- RT
- NSAP
- SIG
- KEY
- PX
- GPOS
- LOC
- NXT (o)
- EID
- NB
- SRV
- ATMA
- NAPTR
- KS
- CERT
- A6
- DNAME
- SINK
- OPT
- APL
- DS
- SSHFP
- IPSECKEY
- RRSIG
- NSEC
- DNSKEY
- DHCID
- NSEC3
- NSEC3PARAM
- HIP
- NINFO
- RKEY
- TALINK
- SPF
- UINFO
- UID
- GID
- TKEY
- TSIG
- IXFR
- AXFR
- MAILB
- MAILA
- DNSSEC

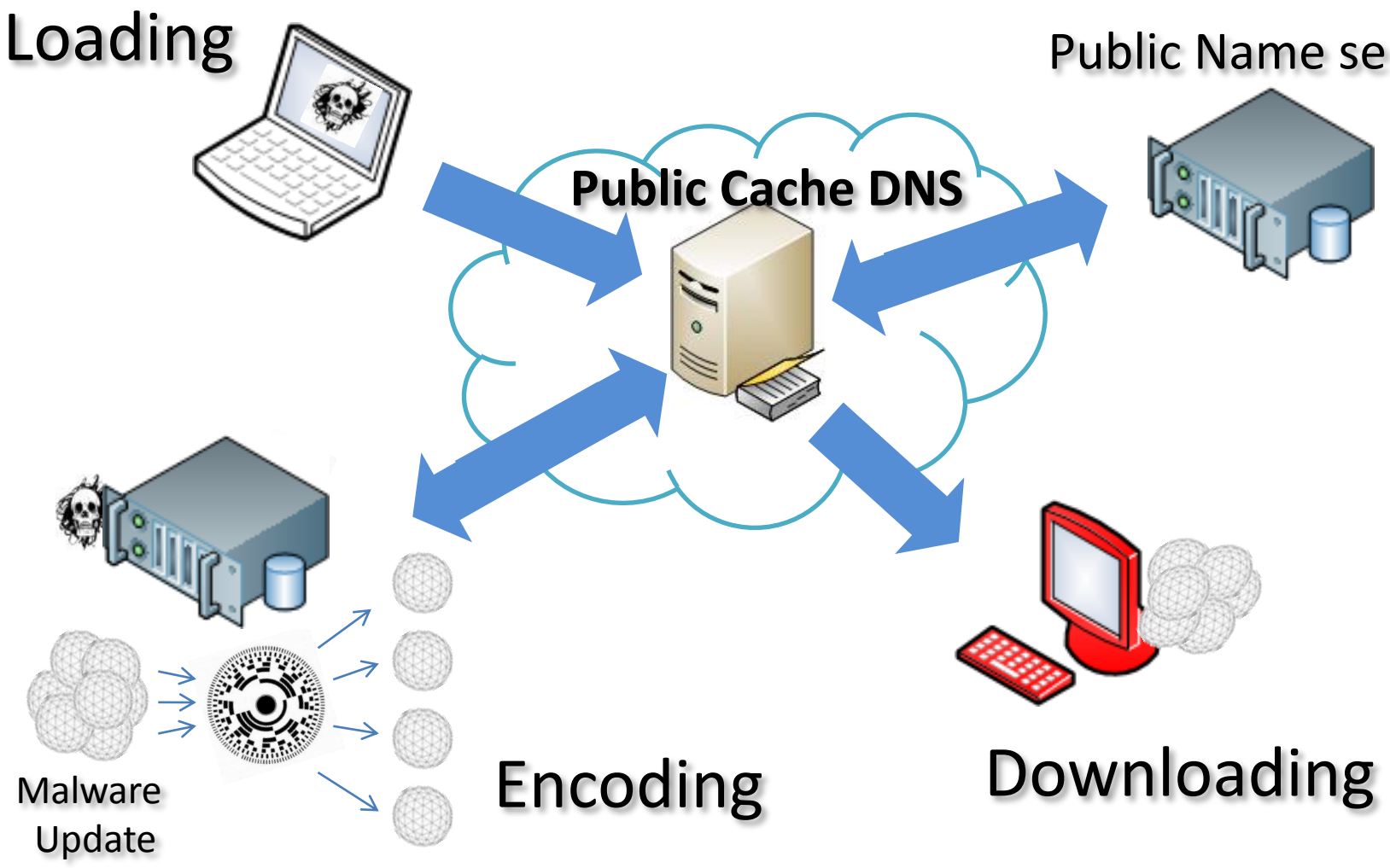


CNAME
Avg. 200 bytes

- 01 Introduction
- 02 DNS in a nutshell
- 03 **Our history**
  - **Implementation**
  - **Improvement**
- 04 Real world
- 05 Results

03 Public DNS Servers

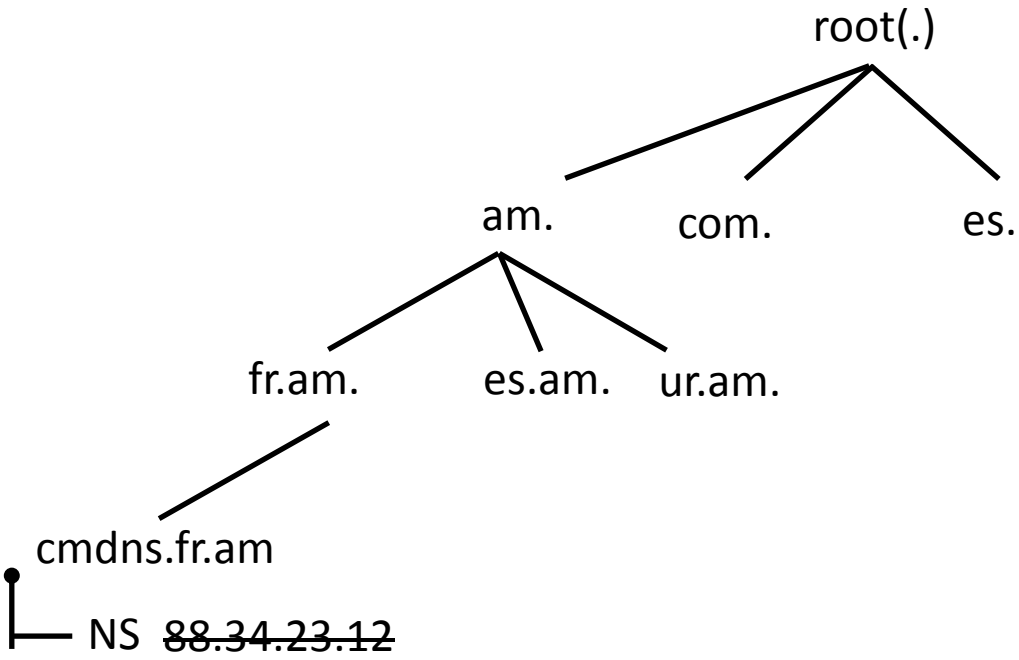
03 Ingredients

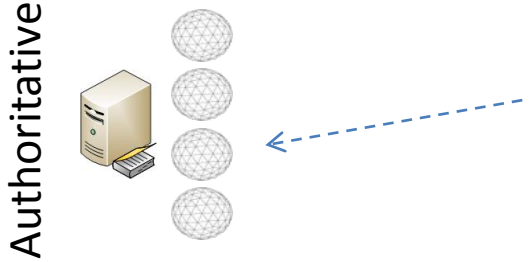


03 Publish process

fr.am		[add]
cmdns.fr.am	NS	nscmd.fr.am
nscmd.fr.am	A	[redacted]

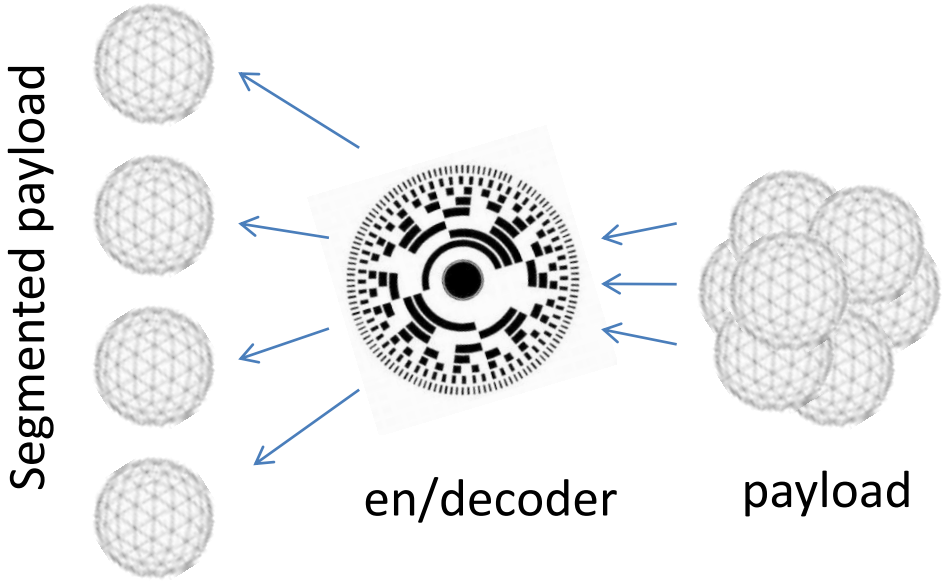
FreeDNS.afraid.org





zoneedit® SITELUTIONS™ Solutions for your site. All in one place. EU.org UNI·CC Network

03 Encoding process

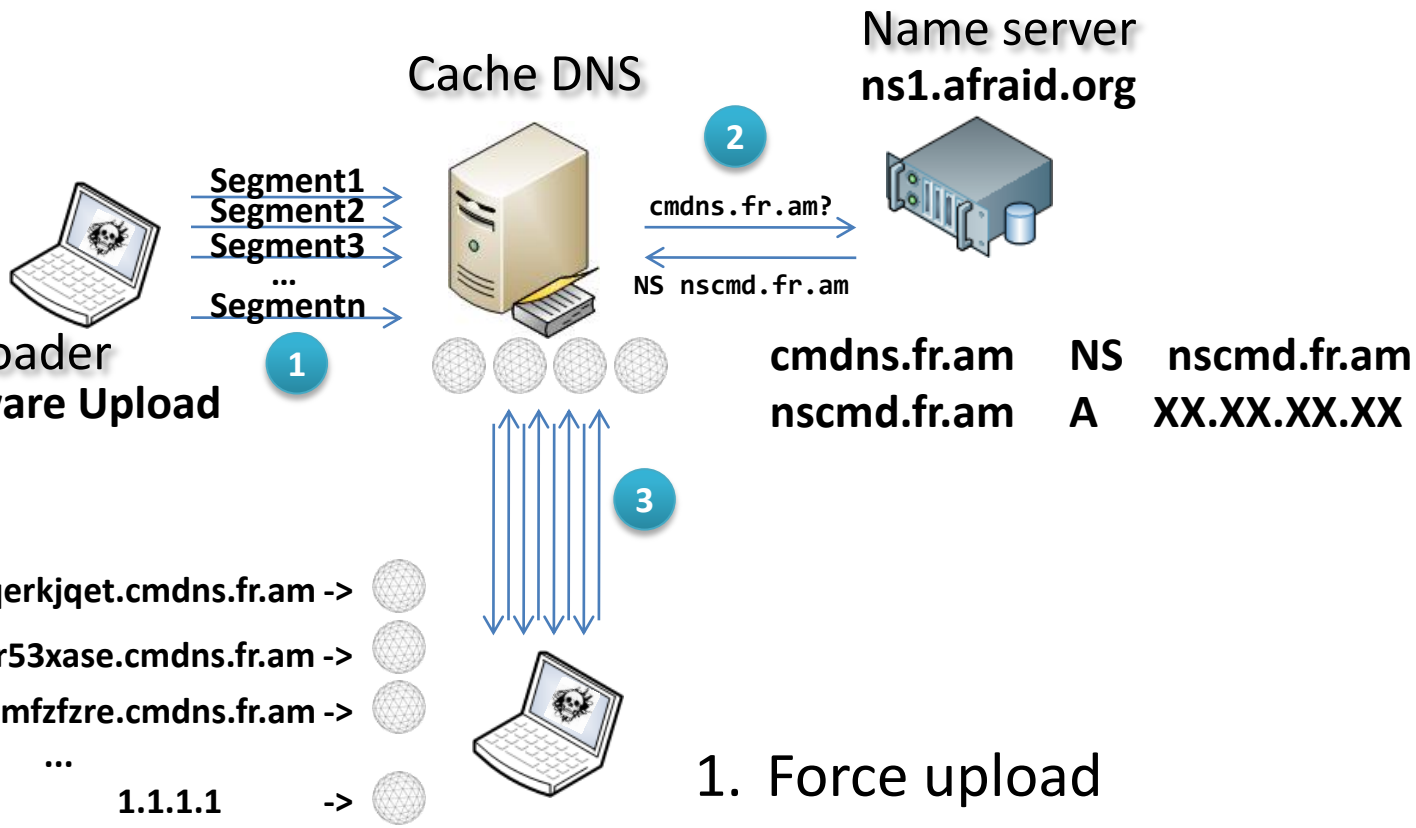


- Compress (gz)
- Base32 Encode
- Split (RFC)
- Become a RR

Resource Record example(*)

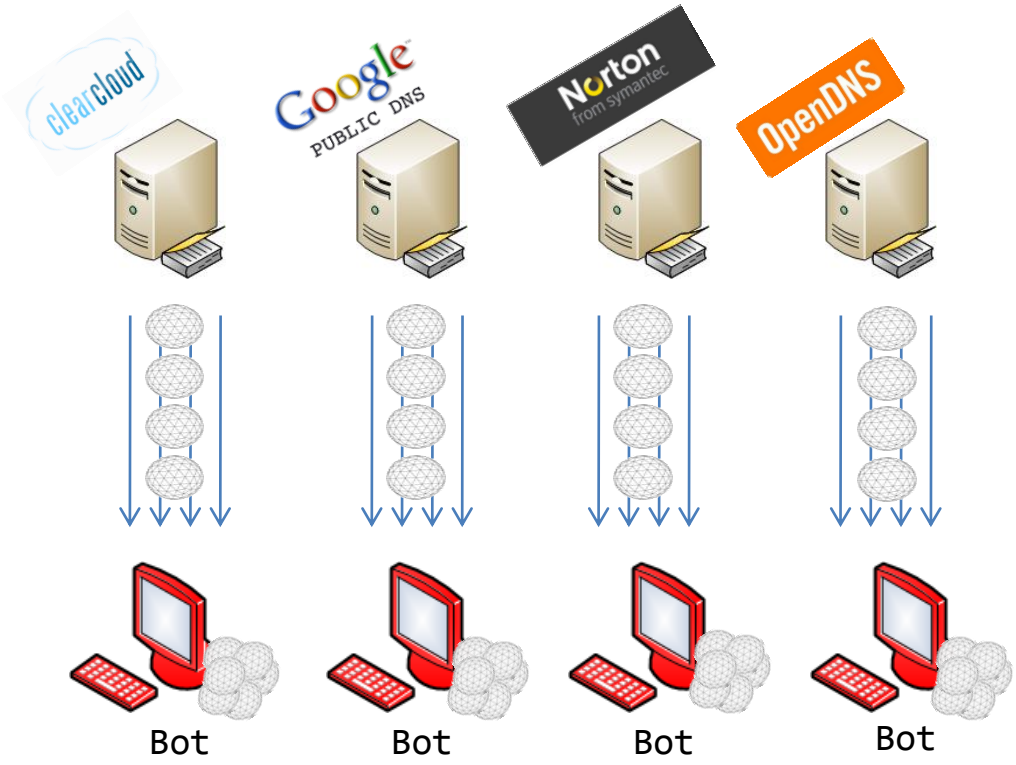
[SegmentedID]	CNAME	[base32EncodeLabel].[subdomain].[domain].[main]
m1-0.cmdns.fr.am.	CNAME	WQ4TOXMQP…N5VSHVOKUEGQ.cmdns.fr.am

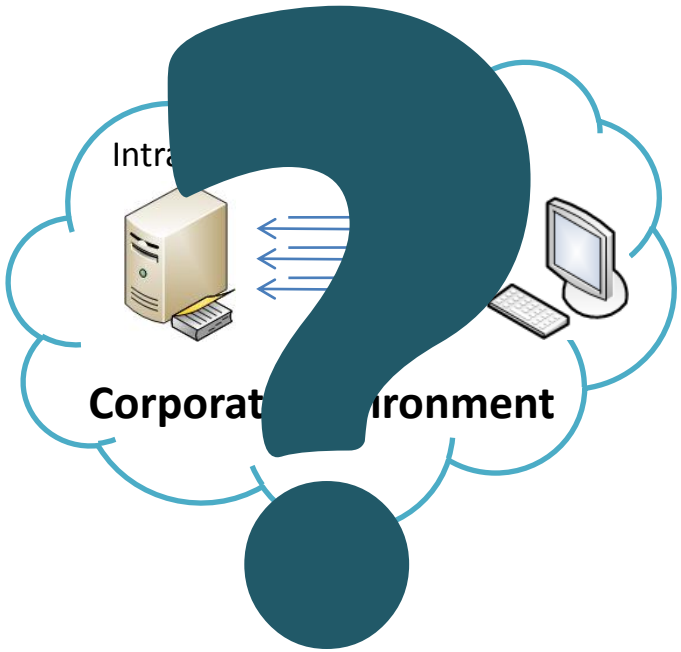
03 Loading process



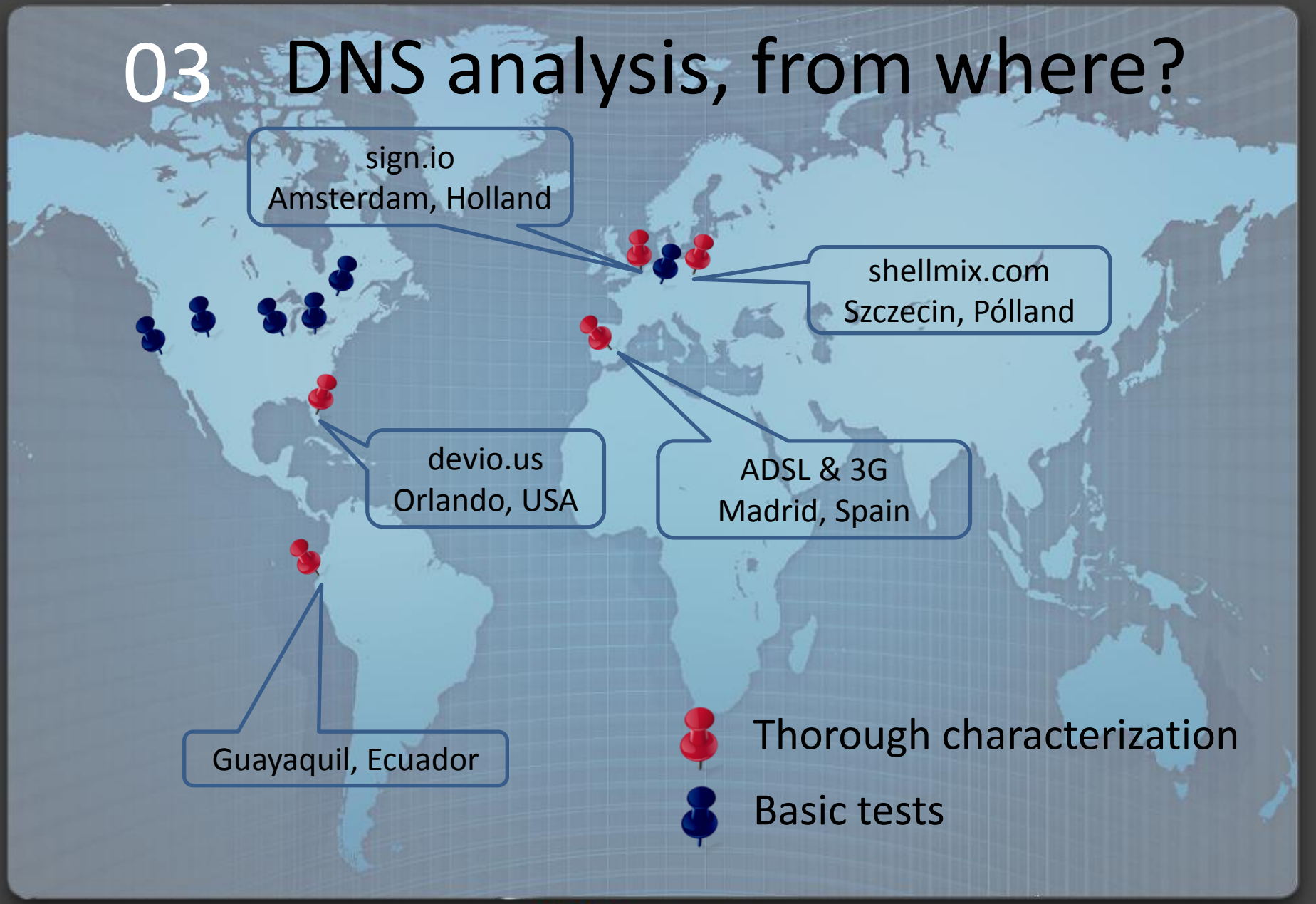
1. Force upload
2. Public NS resolution
3. Cache DNS store segments

03 Downloading process





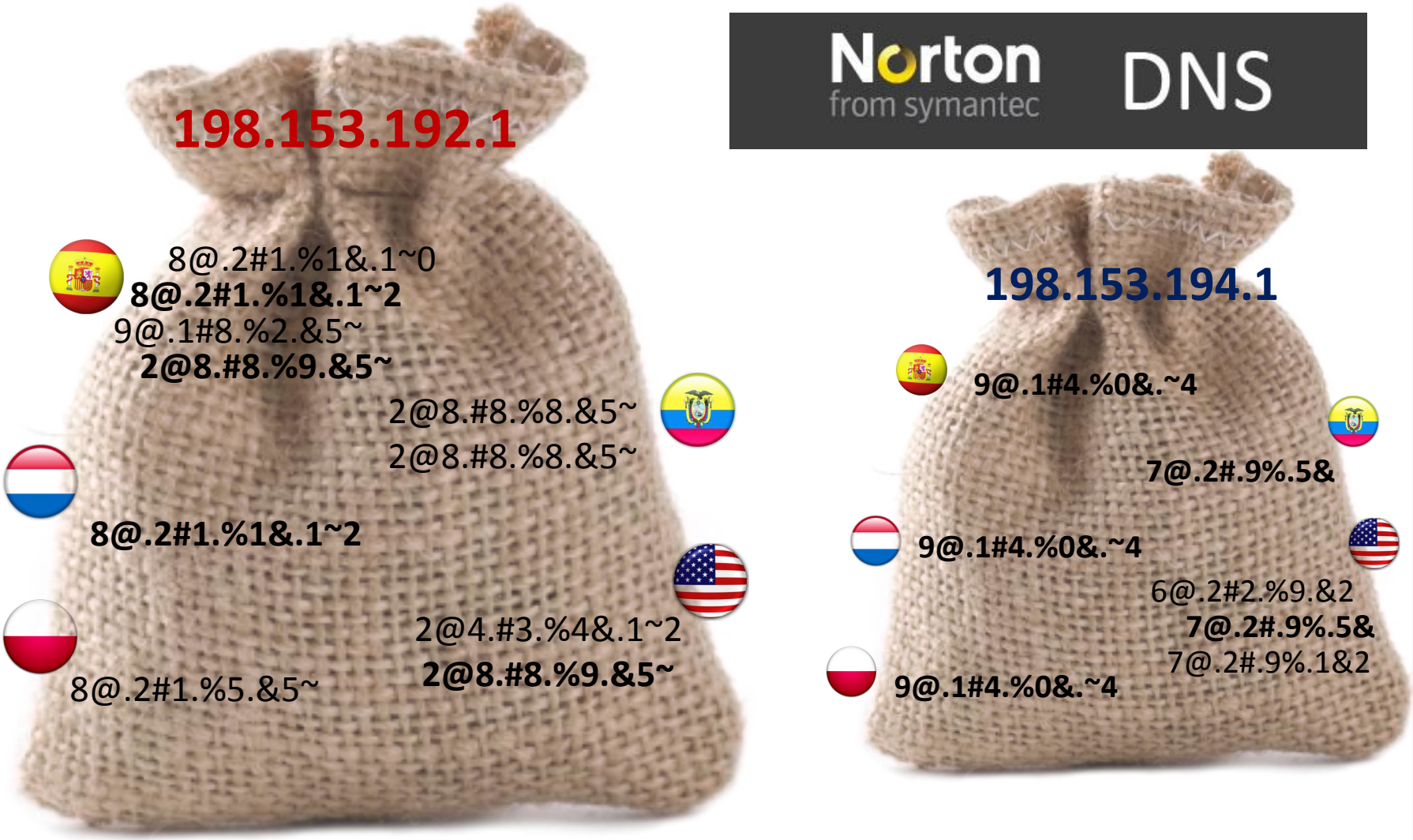
03 DNS analysis, from where?



03 DNS cache survey

- Different locations.
  - IP anycast (DNS proxy):
    - Different locations →Different results.
- Different authoritative DNS.
  - cmdns.mooo.com; cmdns.h4ck.me; cmdns.pocho.cl; cmdns.fr.am; cmdns.m3th.org; cmdns.t28.net; Etc.
- Being patient (thorough characterization)
  - It takes time to run two hundred thousand queries per DNS cache and per location.
- In this study we undertook the task to obtain the list of emitters behind each IP anycast.

03 Characterization (I)



03 Characterization (II)

03 Characterization (III)

8.8.8.8 & 8.8.4.4

Google™ PUBLIC DNS

2@9.#5.%2&.8~ 2@9.#5.%2&.8~ 2@9.#5.%2&.8~
2@9.#5.%2&.8~ 2@9.#5.%2&.8~ 2@9.#5.%2&.8~
2@9.#5.%2&.8~ 2@9.#5.%2&.8~ 2@9.#5.%2&.8~
2@9.#5.%2&.8~ 2@9.#5.%2&.8~ 2@9.#5.%2&.8~
7@.1#5.%8.&0 7@.1#5.%8.&1 7@.1#5.%8.&2
7@.1#5.%8.&3 7@.1#5.%8.&4 7@.1#5.%8.&5
7@.1#5.%8.&6 7@.1#5.%8.&7 **7@.1#5.%6.&0**
7@.1#5.%6.&1 **7@.1#5.%6.&2** **7@.1#5.%6.&3**
7@.1#5.%6.&4 **7@.1#5.%6.&5** **7@.1#5.%6.&6**
7@.1#5.%6.&7 **7@.1#5.%8.&0** **7@.1#5.%8.&1**
7@.1#5.%8.&2

7@.1#5.%6.&0 7@.1#5.%6.&1
7@.1#5.%6.&2 7@.1#5.%6.&3
7@.1#5.%6.&4 7@.1#5.%6.&5
7@.1#5.%6.&6 7@.1#5.%6.&7
7@.1#5.%8.&0 7@.1#5.%8.&1
7@.1#5.%8.&2

03 Characterization (IV)

8.8.8.8 & 8.8.4.4

Google™ PUBLIC DNS

2@9.#5.%2&.8~ **2@9.#5.%2&.8~**
2@9.#5.%2&.9~ 6@.#3%.1&8.~3
6@.2#3.%6&.8~ 6@.#3%.1&8.~5
7@.1#5.%1&.8~ 7@.#2%.1&2.~5
7@.1#5.%1&.8~ **7@.#2%.1&4.~4**
7@.1#5.%5&.8~ **7@.#2%.1&6.~0**
7@.1#5.%5&.8~ **7@.#2%.1&6.~2**
7@.1#5.%5&.8~ **7@.#2%.1&8.~1**
7@.1#5.%5&.8~ **7@.#2%.1&8.~3**
7@.1#5.%5&.8~ **7@.#2%.1&8.~5**
7@.1#5.%5&.8~ **7@.#2%.1&8.~7**
7@.1#5.%4.&0 **7@.1#5.%4.&1** **7@.1#5.%4.&2**
7@.1#5.%4.&3 **7@.1#5.%4.&4** **7@.1#5.%4.&5**
7@.1#5.%4.&6 **7@.1#5.%4.&7** **7@.1#5.%6.&0**
7@.1#5.%6.&1 **7@.1#5.%6.&2** **7@.1#5.%6.&3**
7@.1#5.%6.&4 **7@.1#5.%6.&5** **7@.1#5.%6.&6**
7@.1#5.%6.&7 **7@.1#5.%6.&8** **7@.1#5.%6.&9**
7@.1#5.56.&0 **7@.1#5.%6.&1** **7@.1#5.%4.&0**
7@.1#5.%4.&1 **7@.1#5.%4.&2** **7@.1#5.%4.&3**
7@.1#5.%4.&4 **7@.1#5.%4.&5** **7@.1#5.%4.&6**
7@.1#5.%4.&7 **7@.1#5.%6.&0** **7@.1#5.%6.&1**
7@.1#5.%6.&2 **7@.1#5.%6.&3** **7@.1#5.%6.&4**
7@.1#5.%6.&5 **7@.1#5.%6.&6** **7@.1#5.%6.&7**
7@.1#5.%0.&5 **7@.1#5.%0.&7** 7@.1#5.%0.&9
7@.1#5.%2.&5 7@.1#5.%2.90

2@9.#5. %2&.80 2@9. #5.%2&.81 2@9. #5.%2&.82 2@9. #5.2&4.83 2@9.#5.%2&.84
2@9.#5. %2&.85 2@9.#5.%2&.86 **2@9. #5.%2&.88** 6@.2#3.&68.80 6@.2#3.%6&.81
6@.2#3.%6&.82 **6@.2#3.%6&.83** **6@.2#3.%6&.84** **6@.2#3.&68.85** 6@.2#3.%6&.86
6@.2#3.%6&.87 7@.1#.2%2.&0 **7@**.1#.2%2.&1 **7@**.1#.2%2.&2 **7@**.1#.2%2.&3
7@.1#.2%2.&4 7@.1#.2%2.&5 7@.1#.2%2.&6 **7@**.1#.2%2.&7 **7@**.1#5.1%2.&0
7@.1#5.%12.81 **7@**.1#5.%12.83 7@.1#5.%1&.84 **7@.1#5.%1&.85** **7@**.1#5.%12.&6
7@.1#5.%14.&0 **7@**.1#5.%1&.82 **7@**.1#.1%6.&0 7@.1#5.%2&.81 7@.1#5.%2&.82
7@.1#5.%54.&0 7@.1#5.%5&.81 7@.1#5.%54.&2 7@.1#5.%5&.83 **7@.1#5.%5&.84**
7@.1#5.%54.&5 7@.1#5.%5&.86 **7@.1#5.%54.&7** **7@.1#5.%5&.80** **74.1#5.%5&.81**
7@.1#5.%56.&2 **7@.1#5.%5&.80** **7@.1#5.%5&.81** **7@.1#5.%5&.82** **7@.1%5.1&8.83**
7@.1#5.%58.&4 **7@.1#5.%5&.85** **7@.1#5.%5&.86** **7@.1#5.%5&.87** **7@.1%5.&4.80**
7@.1#5.%4.&1 **7@.1#5.%4.&2** **7@.1#5.%4.&3** **7@.1#5.%4.&4** **7@.1#5.%4.&5**
7@.1#5.%4.&6 **7@.1#5.%4.&7** **7@.1#5.%6.&0** **7@.1#5.%6.&1** **7@.1#5.%6.&2**
7@.1#5.%6.&3 **7@.1#5.%6.&4** **7@.1#5.%6.&5** **7@.1#5.%6.&6** **7@.1#5.%6.&7**
7@.1#5.%6.&8 **7@.1#5.%6.&9** **7@.1#5.%6.&0** **7@.1#5.%6.&1** 7@.1#5.%2.&0
7@.1#5.%2.&1 7@.1#5.%2.&2 7@.1#5.%2.&3 7@.1#5.%2.&4 7@.1#5.%2.&5
7@.1#5.%2.&6 7@.1#5.%2.&7 **7@.1#5.%4.&0** **7@.1#5.%4.&1** **7@.1#5.%4. &2**
7@.1#5.%4.&3 **7@.1#5.%4.&4** **7@.1#5.%4.&5** **7@.1#5.%4.&6** **7@.1#5.%4.&7**
7@.1#5.%6.&0 **7@.1#5.%6.&1** **7@.1#5.%6.&2** **7@.1#5.%6.&3** **7@.1#5.%6.84**
7@.1#5.%6.&5 **7@.1#5.%6.&6** **7@.1#5.%6.&7** 7@.1#5.%6.&1 7@.1#5.%0.&0
7@.1#5.%0.&1 7@.1#5.%0.&2 7@.1#5.%0.&3 7@.1#5.%0.&4 **7@.1#5.%0.&5**
7@.1#5.%0.&6 **7@.1#5.%0.&7** 7@.1#5.%0.&8 **7@**.1#5.%2.80 7@.1#5.%2.&1
7@.1#5.%2.&2 7@.1#5.%2.&3 7@.1#5.%2.&4 **7@.1#5.%2.85** 7@.1#5.%2.86
7@.1#5.%2.&7 **7@**.1#5.%4.&0 7@.1#5.%4.81 7@.1#5.%4.82 7@.1#5.%4.83 7@.1#5.%4.84
7@.1#5.%4.85 7@.1#5.%4.86 7@.1#5.%4.87

03 Preliminary results

03 Characterization (V)

ns2.cisco.com (64.102.255.44) emitters

6@.1#4.2%5.&2
6@.1#2.2%5.&3
6@.1#2.2%5.&0
6@.1#2.2%5.&1

BT MDIP Dynamic Address Pools and Infrastructure
indnsc70.bt.net (**62.6.40.162**) **open emitter**

ns.above.net
(**207.126.96.162**)
open emitter

MarkosWeb (Private World Communications)
cache1.dnsresolvers.com
(**205.210.42.205**) **open emitter**

03 Preliminary results

03 Theory Vs. Reality

- DNS pools:
  - Load on each DNS in pool.
  - Load on more than one DNS pool.
  - Complex retry logic.
- Limited in corporative environments.
- Malware source must disappear before the first download.
- Must use client default DNS settings.

03 Improvement

- Need another way.
- Maybe can use three party resources …

- … Use Cache DNS as authoritative server.
  - Malware source can disappear.
  - Completely asynchronous communication.
  - Origin trace is little more difficult.
  - Needed only one load process.

IMPORTANTE COMPAÑÍA ESPECIALIZADA EN DISTRIBUCIÓN DE MALWARE SELECCIONA

SERVIDORES DNS (OPEN EMITTERS)

Se requiere:

- Accesibilidad a nivel mundial
- Admitir y resolver correctamente preguntas recursivas (funcionalidad *open resolver*)
- Sin limitaciones a la hora de almacenar nuevos registros de cualquier tipo (funcionalidad de caché)
- Experiencia en trabajar con TTL altos (mínimo 86.400 segundos)
- Capacidad para aceptar responsabilidades:
  - Respondiendo a consultas no recursivas (+norecurse)
  - Respondiendo con autoridad: Marcando las respuestas como autoritativas (bit AA) independientemente del dominio por el que pregunten (tenga autoridad sobre el o no)
- Se valorarán estabilidad y altas prestaciones

Interesados enviar dirección IP a cmd@iniqua.com

03 Finding Nemo (I)

380.700
Open emitters

15.553.600
Speak the DNS protocol

11.920.500
Open resolvers

IPv4 addresses: 256^4 = 4.294.967.296
IPv4 addresses routed on the Internet: 2.126.357.495
http://dns.measurement-factory.com/surveys/201010/

03 Finding Nemo (II)

10,9 % name servers .com, .net & .org
Open emitters

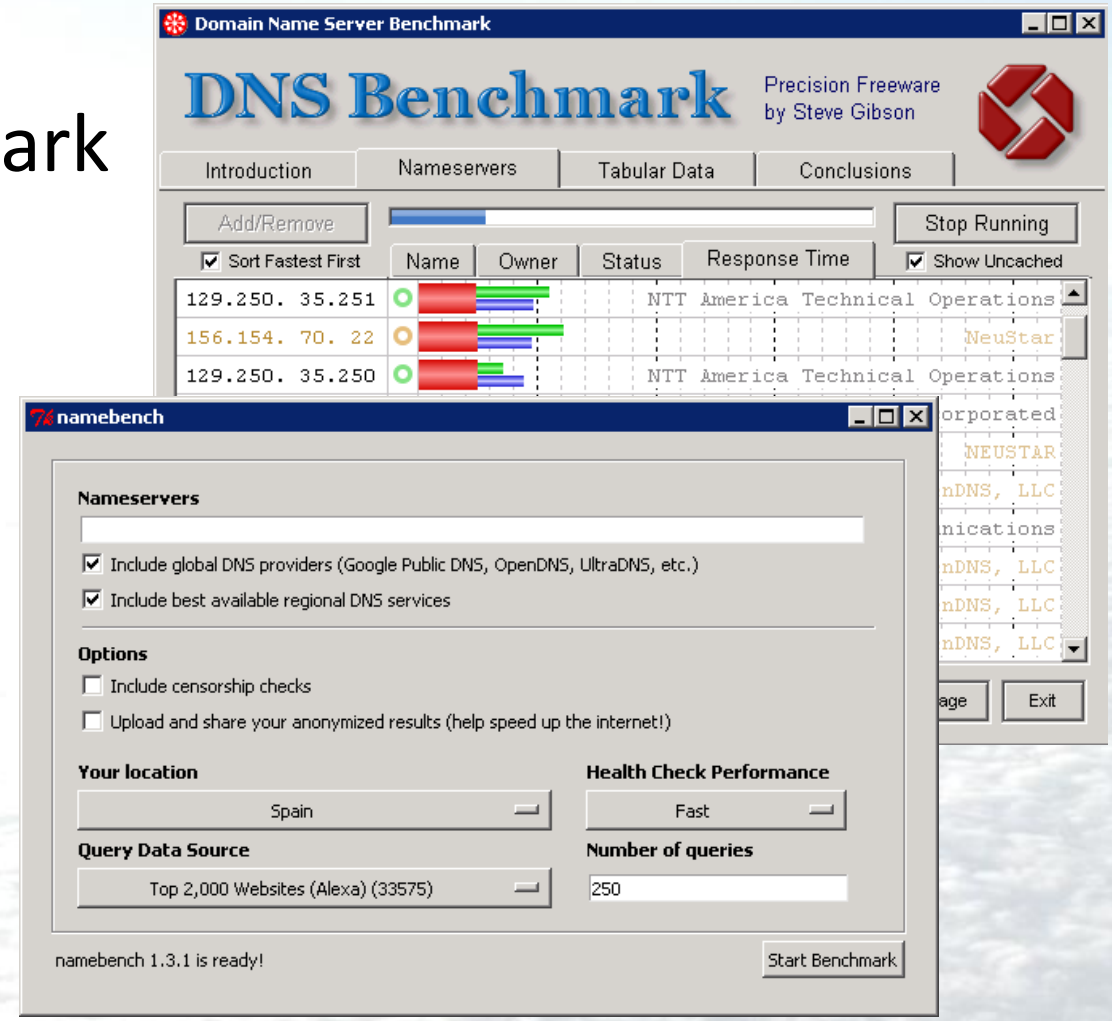
13,4 million domains

8,6 million domains

90 million domains

03 Free public DNS servers list

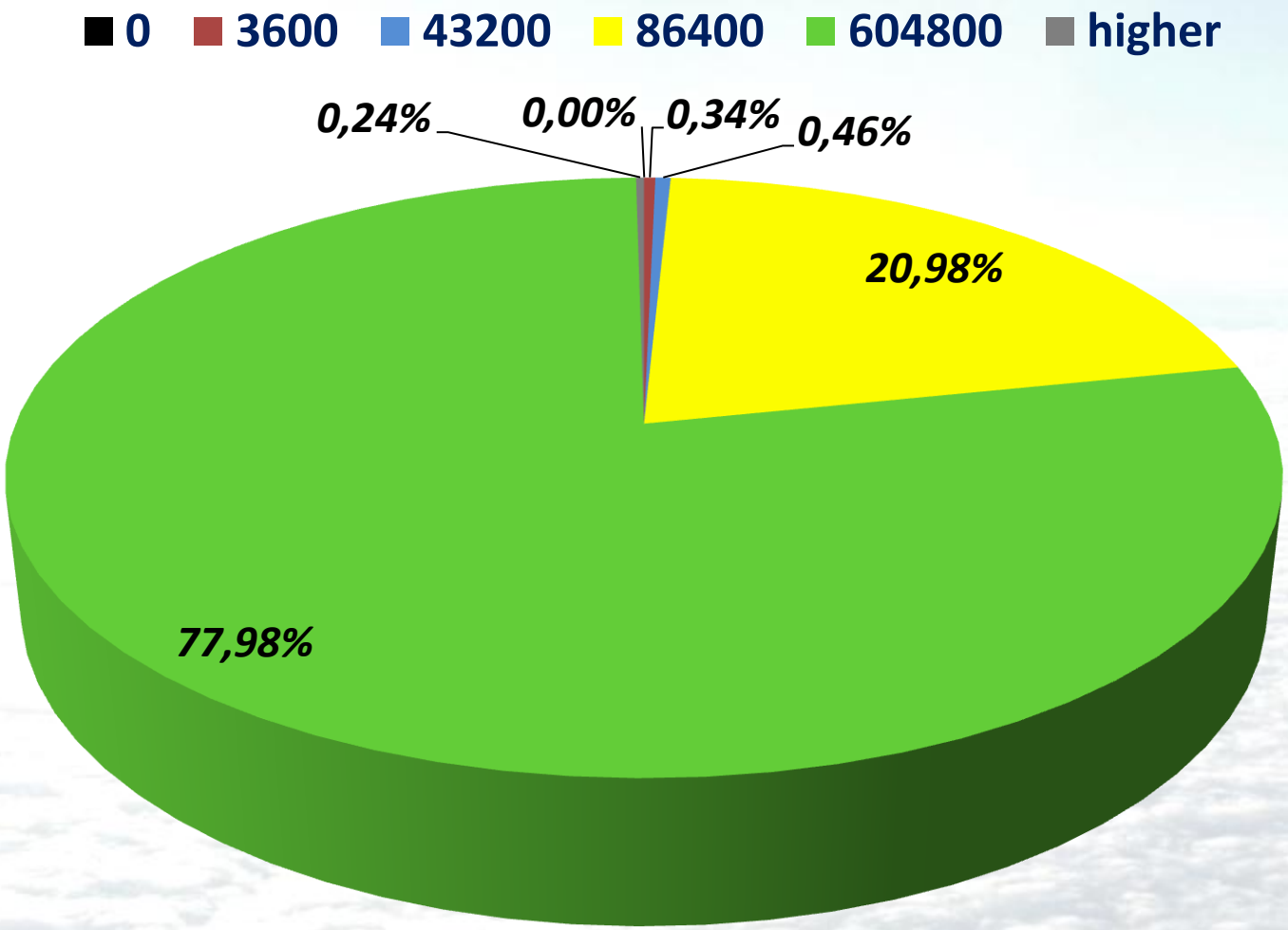
- DNS Benchmark
- namebench
- chaz6.com



03 Searching for good emitters

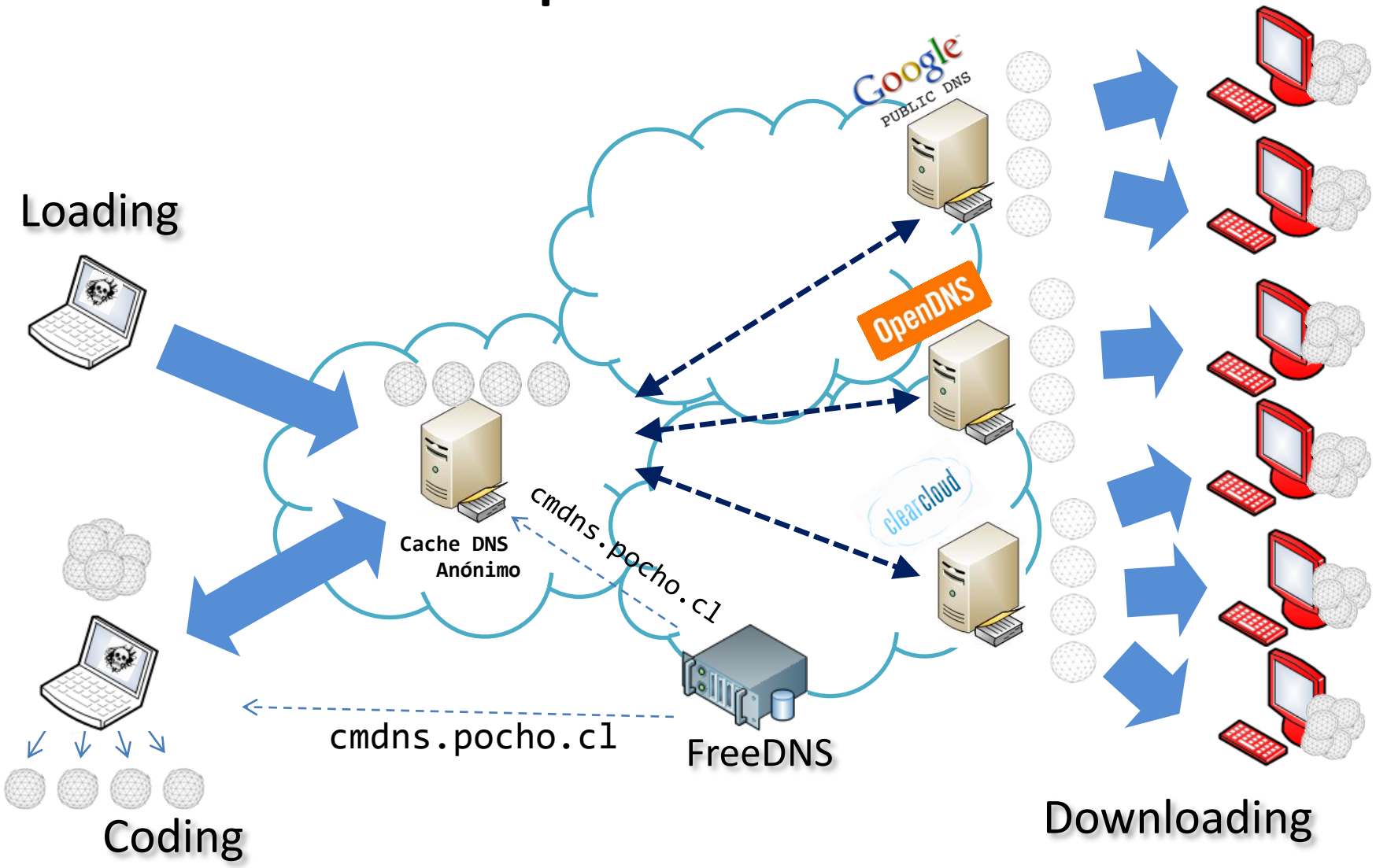
February 2011	From Spain		From USA
Queried hosts	10.406		10.406
Replying hosts	9.077		9.094
Open resolvers	6.941		7.028
Open emitters	5.243	5.175	5.214
Accept +norecurse queries	5.075	5.005	5.047
TTL ≈ 604800	3.908	3.905	3.905

03 Here they are, in all their glory



Maximum TTL Value

03 New process overview



- 01 Introduction
- 02 DNS in a nutshell
- 03 Our history
  - Implementation
  - Improvement
- 04 Real world
- 05 Results

04 Here and right now (I)

scsnms.switch.ch (130.59.10.30 y 130.59.1.30)
ns02.fccn.pt (193.136.2.228)
ns15.communitydns.net (194.0.1.15)
- DNS route
sun.rediris.es (130.206.1.2)
- DNS route
chico.rediris.es (130.206.1.3)
- DNS route
mirzam.ccc.upv.es (158.42.1.5)
- DNS route
vega.cc.upv.es (158.42.4.1)
- DNS route

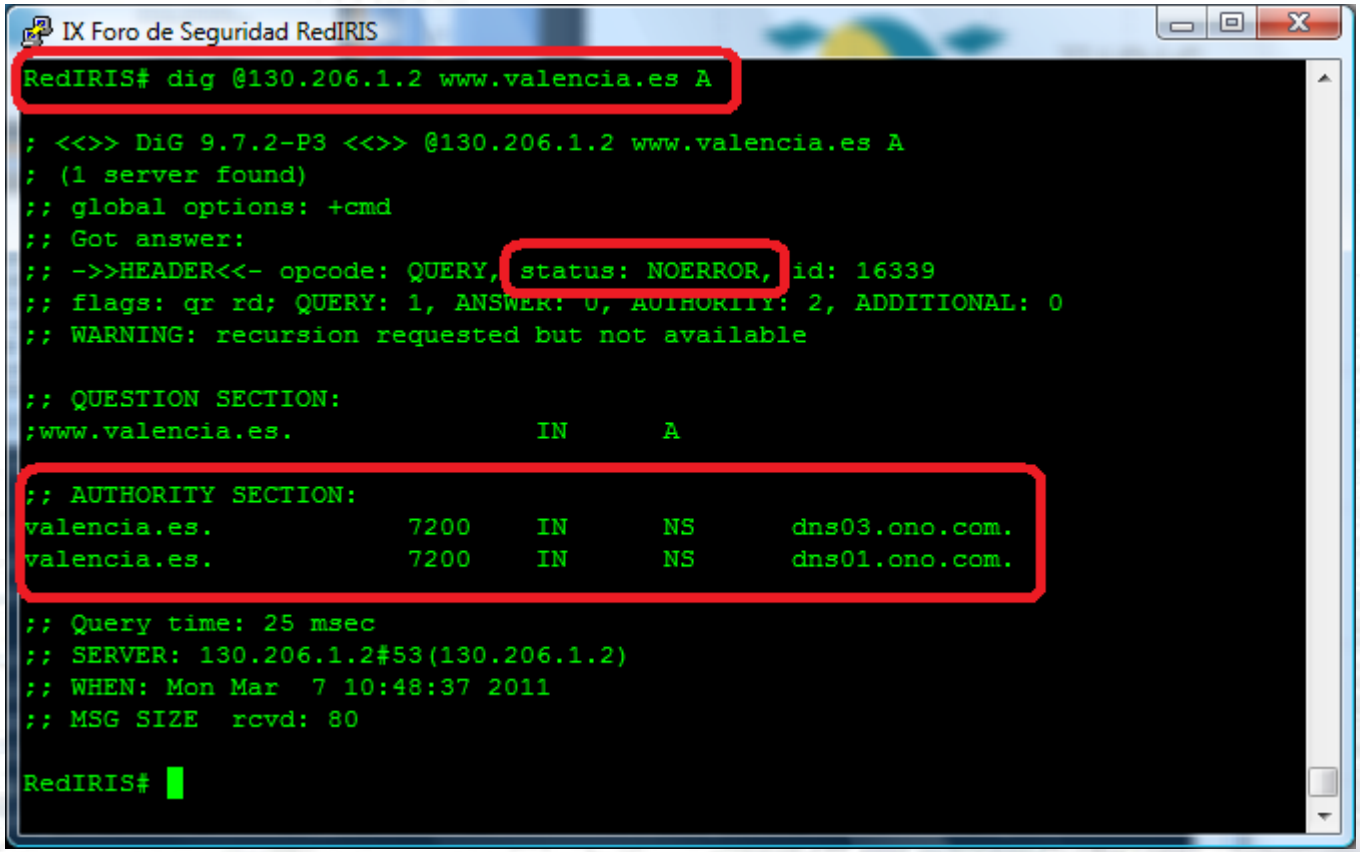
nso.nic.es (194.69.254.2)
ns1.s2grupo.com (62.97.78.23)

ns.gesdatos.com (212.101.64.37)
- recursion is enabled
- open emitter
- DNS caché (TTL 604800 s)
- +norecurse (allowed)

dns3.servicom2000.com (212.101.72.4)
dns2.servicom2000.com (212.101.64.4)

04 Here and right now (I)

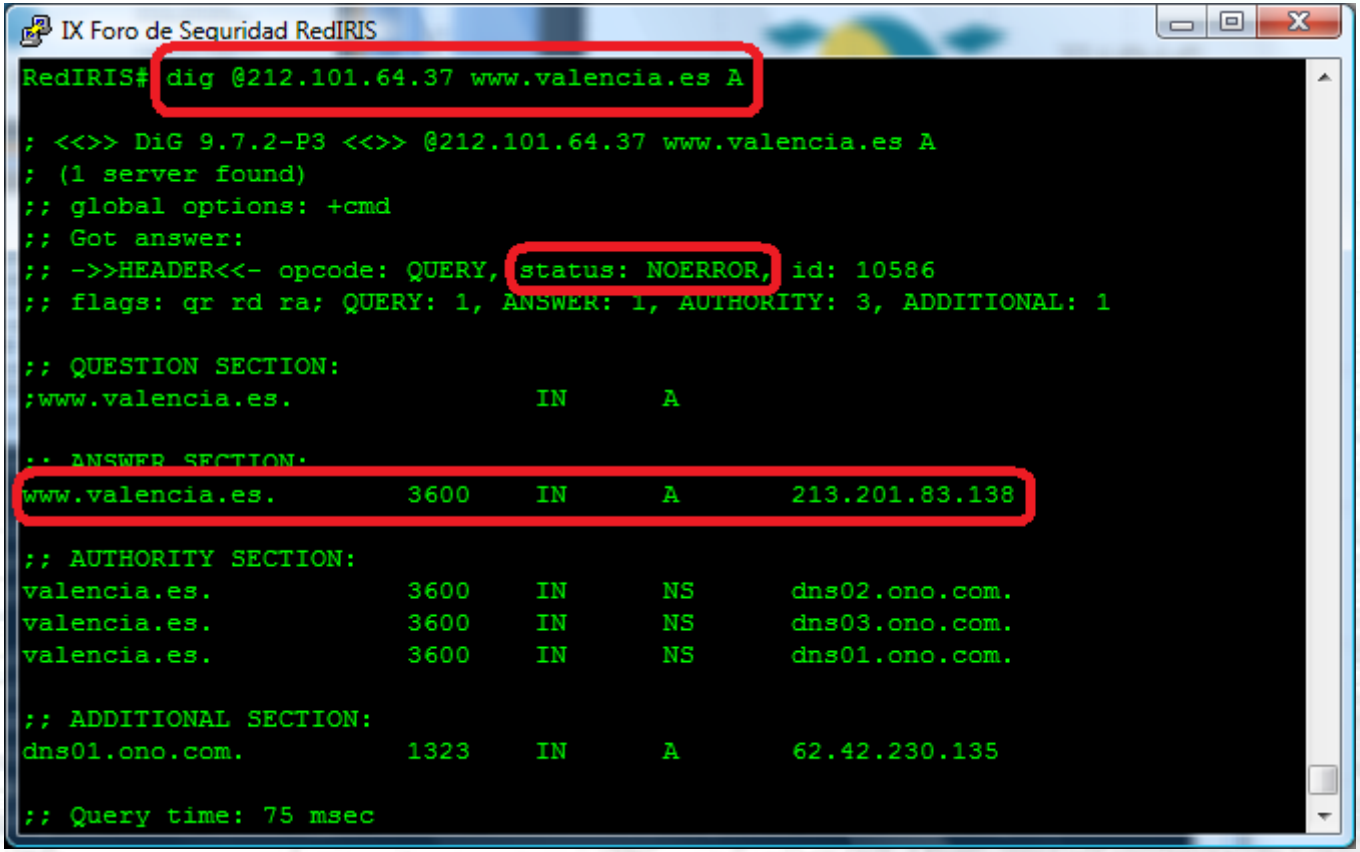
sun.rediris.es (130.206.1.2)
- DNS route



04 Here and right now (I)

GESDATOS ENS

ns.gesdatos.com (212.101.64.37)
- DNS caché (open emitter)



04 Here and right now (II)

- **Analyzing 76 domains related to universities with presence in Spain** (188 different name servers)**:**
  - **31** Authority Servers accept recursive queries (**open resolvers**).
  - **29 of then are DNS cache & open emitters**.
    - +norecurse allowed.
  - **TTL value for 23 is 604.800 seconds** (86.400 seconds for the others six).

04 Here and right now (III)

- **Analyzing 131 domains related to banks with presence in Spain** (145 different name servers)**:**
  - **32** Authority Servers accept recursive queries (**open resolvers**).
  - **21 of then are DNS cache & open emitters**.
    - +norecurse allowed.
  - **TTL value for 14 is 604.800 seconds** (86.400 s for 6 and 172.800 s for the other one).

04 PoC (I)

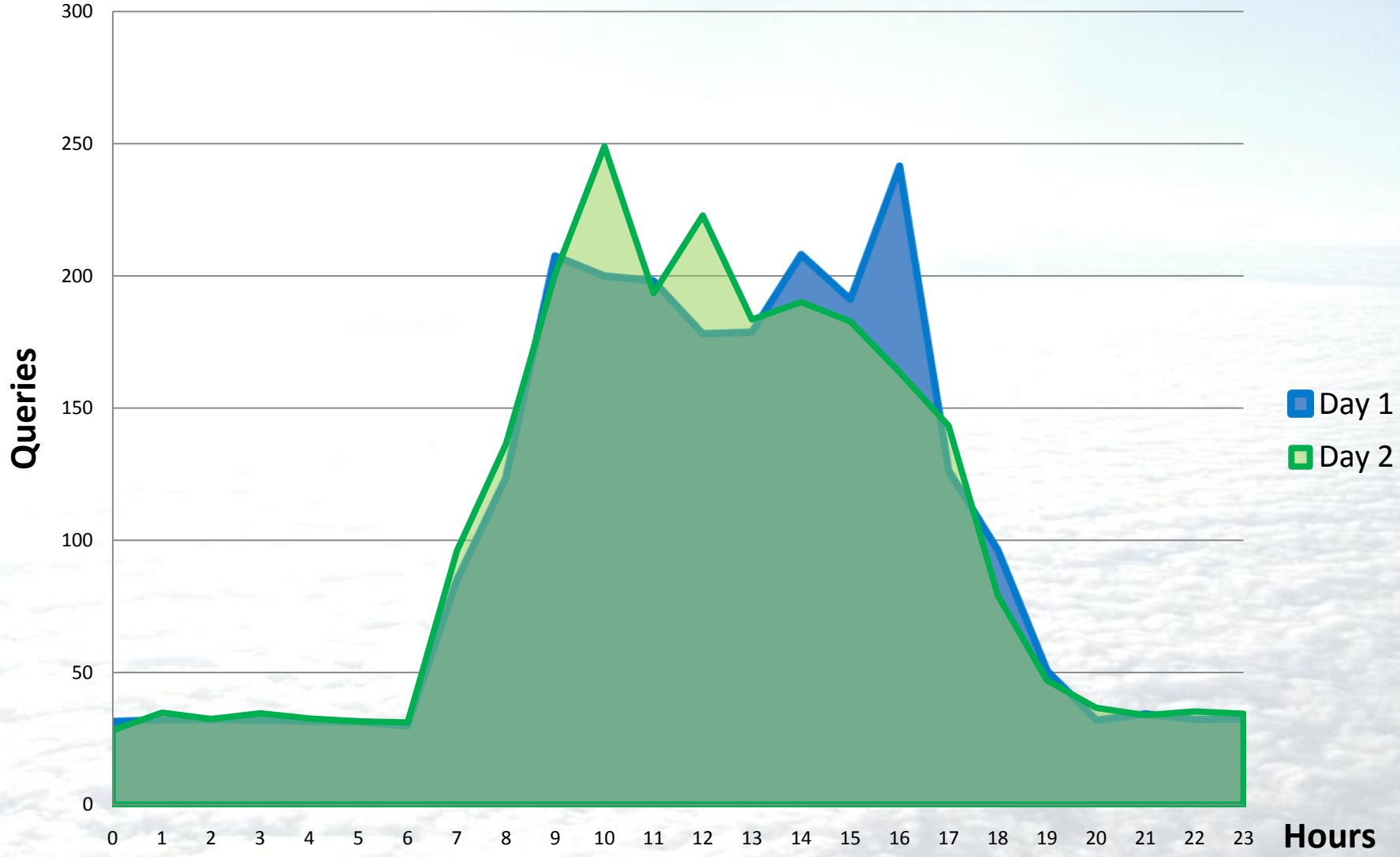
- Sample files (¬malware):
  - nc (20.156 bytes)
  - diff (100.324 bytes)
- Domain to be used: “cmdns.pocho.cl”
- Selected servers (TTL: 604.800 s):
  - 2@7.#2%.9&.1~2
  - 1@3.#3%.2&6.1~
- From 20th Feb to 26th Feb, 2011

04

PoC (II)

File	nc		diff	
Size	20.156 bytes		100.324 bytes	
Queries needed	44 (2.24 queries/KB)		222 (2.27 queries/KB)	
Upload time	Spain			
2@7.#2%.9&.1~2	33 s		2 min 27 s	
1@3.#3%.2&6.~1	18 s		1 min 20 s	
Download time (First time)	Spain	USA	Spain	USA
Google (8.8.8.8)	10 s	11 s	38 s	2 min 35s
Norton (198.153.192.1)	12 s	28 s	52 s	2 min 17s
OpenDNS (208.67.222.222)	25 s *	25 s *	1 min 29 s *	1 min 51s *
Intranet (X.X.X.X)	22 s *	-	1 min 28 s *	-

04 User DNS traffic



04 Live demo (I)

Sample files	Bytes	Queries needed	VIRUS TOTAL
m1: PHP-Backdoor “id”	498	2	24/43
m2: “IE-KillProgramsTab.exe”	10.240	18	40/43
m3: PHP bot “pbot.txt”	23.140	21	28/43
m4: KillAV “ep.exe”	31.604	114	19/43
m5: Zeus binary “bot.exe”	152.064	636	29/41
m6: Trojan SpyEye “seye.exe”	200.704	535	32/43

04 Live demo (II)

Domains to be used	Selected servers (Open Emitters)	TTL Seconds
cmdns.mooo.com	1@0.#1%.1&7.~	604.800
cmdns.m3th.org	2@2.#6.%4.&6 2@2.#6.%4.&7	604.800
cmdns.h4ck.me	2@2.#0%.6&.3~	604.800
cmdns.fr.am	2@7.#5.%2.&	604.800
cmdns.t28.net	1@5.#4%.2&8.~3	604.800
cmdns.pocho.cl	2@7.#2%.9. &6~ 1@3.#3%.2&6.~1	604.800

- All domains were loaded 7th March ➔ on air until 14th March.
  - Try it: ***dig m1-0.cmdns.pocho.cl A***

04 Repair

Uhmmm rate-limiting queries!!!!!!

The first 100 queries: 48 s
200 queries: 4 min 4 s
300 queries: 9 min 4 s
400 queries: 13 min 54 s
500 queries: 18 min 33 s
600 queries: 23 min 52 s

			bot.exe (m5)	
Si			152.064 bytes	
			28 queries/KB)	
Up			S	
2				s
Down		Ecuador	Spain	Ecuador
	s	18 s	22 min 8 s *	25 min 36 s *
Norton (198.153.192.1)	5 s	12 s	2 min 26 s	5 min 18 s
OpenDNS (208.67.222.222)	5 s **	10 s **	3 min 4 s **	5 min 47 s **
Intranet (X.X.X.X)	6 s **	-	1 min 19 s**	-
Universitat Politècnica de València (158.42.250.195)	3 s	-	1 min 32 s	-

04 The Origin of Evil

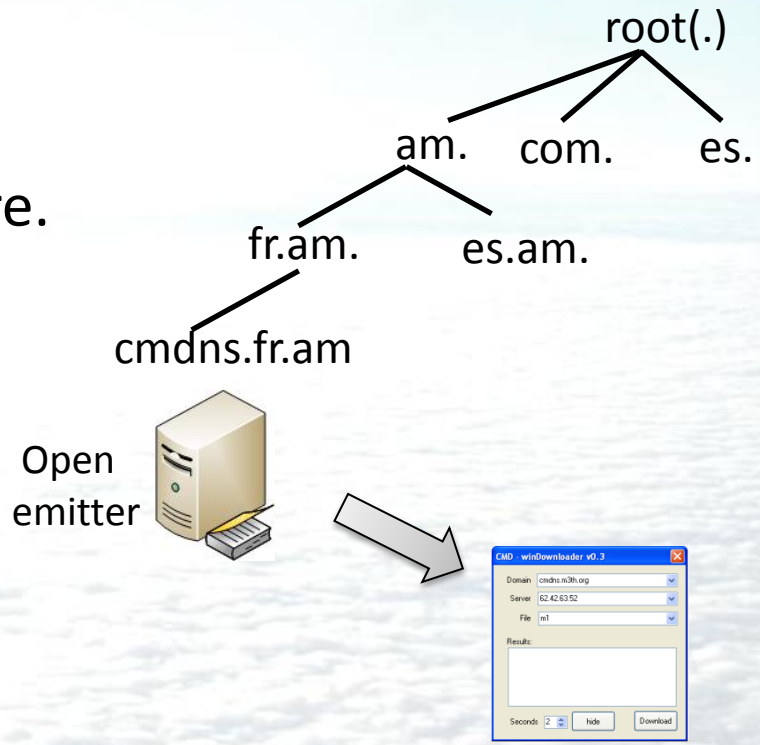
CMD - RedIRIS 2011

```
RedIRIS# dig m1-0.cmdns.h4ck.me A

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> m1-0.cmdns.h4ck.me A
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28983
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;m1-0.cmdns.h4ck.me.            IN      A

;; ANSWER SECTION:
m1-0.cmdns.h4ck.me.     594616  IN      CNAME   D6FQQCEMLNQE2AADNUYQANORZFXJWQAAQDQXXJF4IMKPLYGKA7
BWAHFDGSVOYAI.DMYZTBNUDF4ITBQ3CSYQQGZT37K3IP7XX572P76W5MTG7HU4PTY3DCI6DZPD4W2.3TGNW3ZNIGIVDX2GSNWK
PE4V75QY4FC4VZCHXYGIAVHDSEDJ6XDOO4IJJPYZASN.cmdns.h4ck.me.
D6FQQCEMLNQE2AADNUYQANORZFXJWQAAQDQXXJF4IMKPLYGKA7BWAHFDGSVOYAI.DMYZTBNUDF4ITBQ3CSYQQGZT37K3IP7XX5
72P76W5MTG7HU4PTY3DCI6DZPD4W2.3TGNW3ZNIGIVDX2GSNWKPE4V75QY4FC4VZCHXYGIAVHDSEDJ6XDOO4IJJPYZASN.cmdn
s.h4ck.me. 594616 IN CNAME WQ4TOXMQP2DVAES3MTGS3ELI5KTOQ6GYV6RLOSYSK3T4N5F5HG6EVSHVOKUEGQW.K2RPYEQ
UYFGFXILVYXSVC7P57V2JNLFJ3RZZFG3LJY6YUHB3M3LK7XPHNNLMQSR.VYHCBVTLGNYB27BA6WET24K7GITFCCZHOBZ2NOVHK
4AIS3URZTU6YTI64ZFRTB4.cmdns.h4ck.me.
WQ4TOXMQP2DVAES3MTGS3ELI5KTOQ6GYV6RLOSYSK3T4N5F5HG6EVSHVOKUEGQW.K2RPYEQUYFGFXILVYXSVC7P57V2JNLFJ3R
ZZFG3LJY6YUHB3M3LK7XPHNNLMQSR.VYHCBVTLGNYB27BA6WET24K7GITFCCZHOBZ2NOVHK4AIS3URZTU6YTI64ZFRTB4.cmdn
s.h4ck.me. 594616 IN A 1.2.3.4

;; AUTHORITY SECTION:
cmdns.h4ck.me.          3477    IN      NS      nscmd.h4ck.me.

;; Query time: 4 msec
;; SERVER: 200.93.221.179#53(200.93.221.179)
;; WHEN: Mon Mar  7 08:44:34 2011
;; MSG SIZE  rcvd: 484
```

- 01 Introduction
- 02 DNS in a nutshell
- 03 Our history
  - Implementation
  - Improvement
- 04 Real world
- 05 Results

05 Results

- Public cache DNS:
  - can be used as a platform to store and distribute malware.
- DNS architecture:
  - is available.
- Implementation:
  - just do it.
- Survey Results:
  - can be used to define countermeasures.



05 Best Current Practice

00

References

http://code.kryo.se/iodine/

http://dns.measurement-factory.com/

http://www.chaz6.com/files/resolv.conf

http://www.grc.com/dns/benchmark.htm

http://darkwing.uoregon.edu/~joe/secprof10-dns/secprof10-dns.pdf

http://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Kaminsky.pdf

http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-kaminsky/bh-us-04-kaminsky.ppt

http://code.google.com/p/namebench/

http://www.pcworld.com/article/220024/feds_accidentally_seize_84000_innocent_domains_link_them_with_child_porn.html

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf

http://www.secdev.org/projects/scapy/

https://www.isc.org/software/bind/documentation/arm95#man.dig

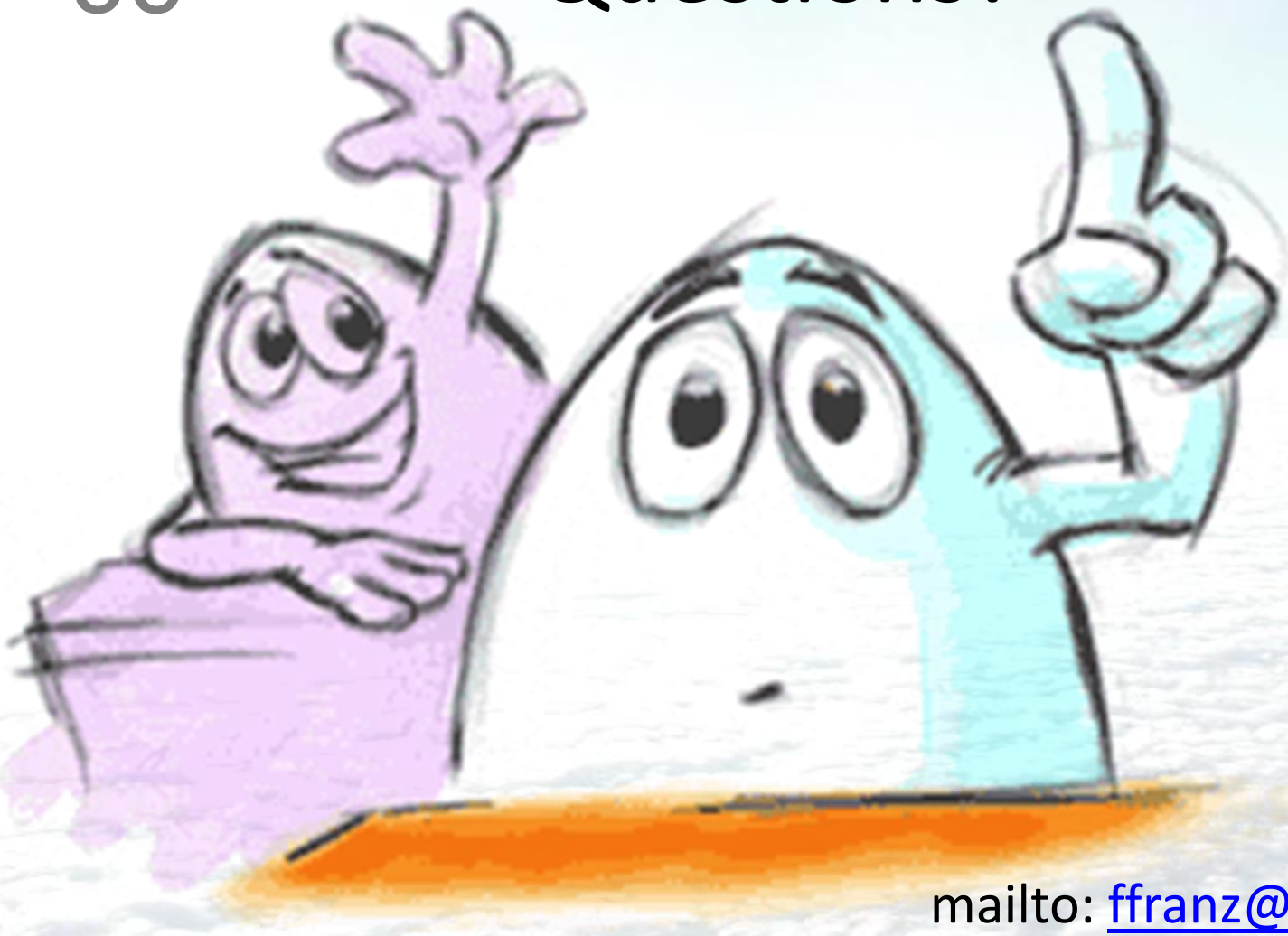
http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl

http://hakin9.org/magazine/1652-mobile-malware-the-new-cyber-threat

http://www.ietf.org/rfc/rfc{1033,1034,1035,1183,2181}.txt

00

Questions?



mailto: ffranz@iniqua.com
mailto: charlie@tid.es

Thanks for your time!