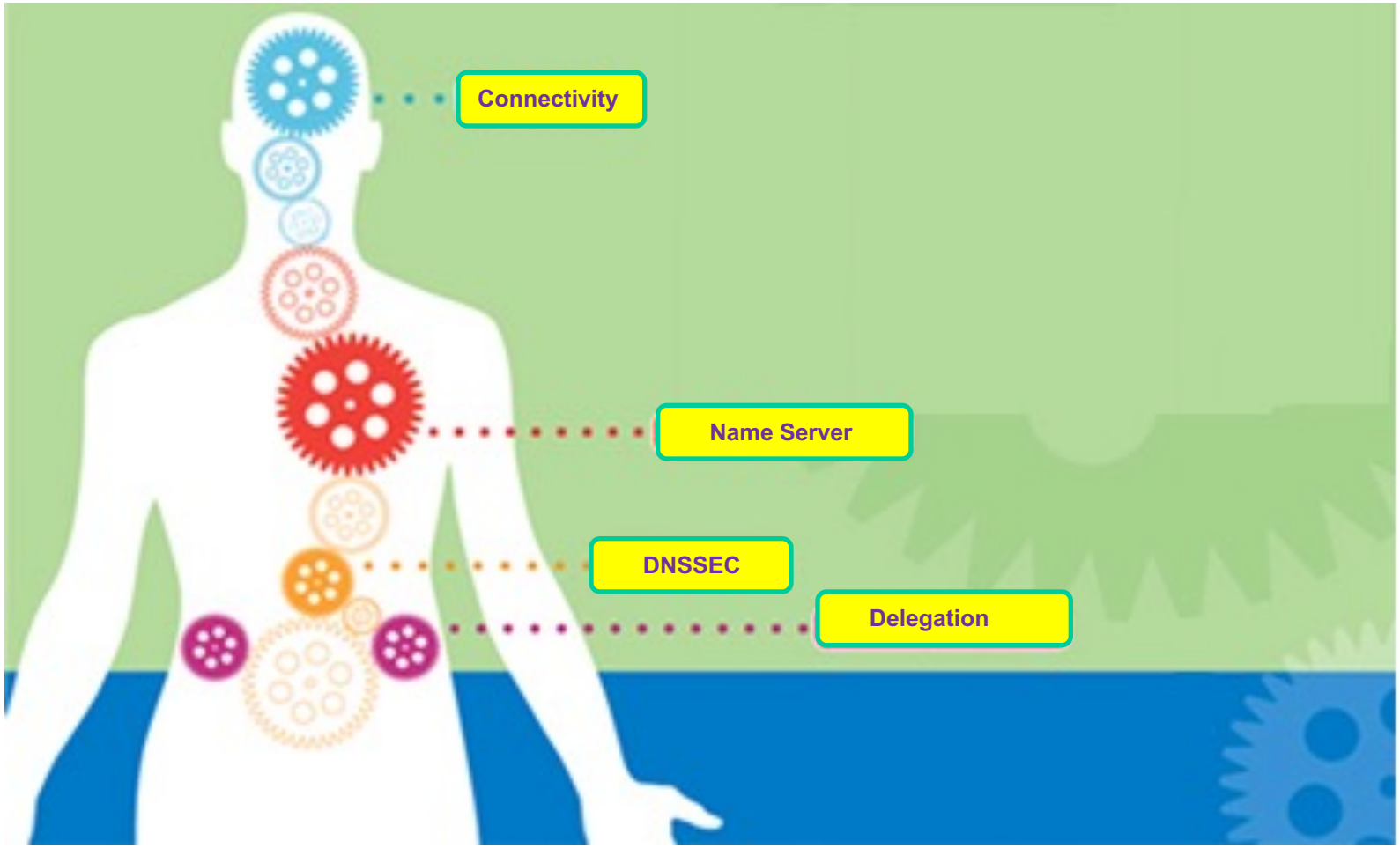
Benchmarking Zonemaster –

Sandoche Balakrichenan (Afnic) & Einar Lonn (IIS)

Health check



DNS Health check



Basic tools

- ✓DNS errors
  - ✓ dig
  - ✓ nslookup

Example with dig

```
$ dig ssi.gouv.fr

; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> ssi.gouv.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36879
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ssi.gouv.fr.                IN      A

;; ANSWER SECTION:
ssi.gouv.fr.          300     IN      A       213.56.166.109

;; AUTHORITY SECTION:
ssi.gouv.fr.          63182   IN      NS      dns1.certa.ssi.gouv.fr.
ssi.gouv.fr.          63182   IN      NS      dns1.ssi.gouv.fr.

;; ADDITIONAL SECTION:
dns1.ssi.gouv.fr.     63182   IN      A       213.56.166.96
dns1.certa.ssi.gouv.fr. 69452 IN      A       213.56.176.3

;; Query time: 26 msec
;; SERVER: 10.10.81.162#53(10.10.81.162)
;; WHEN: Wed May 27 14:54:34 CEST 2015
;; MSG SIZE  rcvd: 132
```

Comprehensive verification of a DNS zone

- ✓Well known tools
  - ✓ ZoneCheck
  - ✓ DNScheck
  - ✓ dnsviz

Example with ZoneCheck

```
$zonecheck ssi.gouv.fr
ZONE  : ssi.gouv.fr.
NS <= : dns1.ssi.gouv.fr. [213.56.166.96]
NS    : dns1.certa.ssi.gouv.fr. [213.56.176.3]
~~~~ |    warning    || ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
w> Nameservers are all part of the same AS
 | Adv: ZoneCheck
 |   To avoid losing all connectivity with the authoritative DNS in case
 | of a routing problem inside your Autonomous System, it is advised to
 | host the DNS on different AS.
 `----- -- -- - -  -
 :   All the nameservers are part of the same Autonomous System (AS number
 : 3215), try to have some of them hosted on another AS.
 `..... .. .. . .  .
=> generic

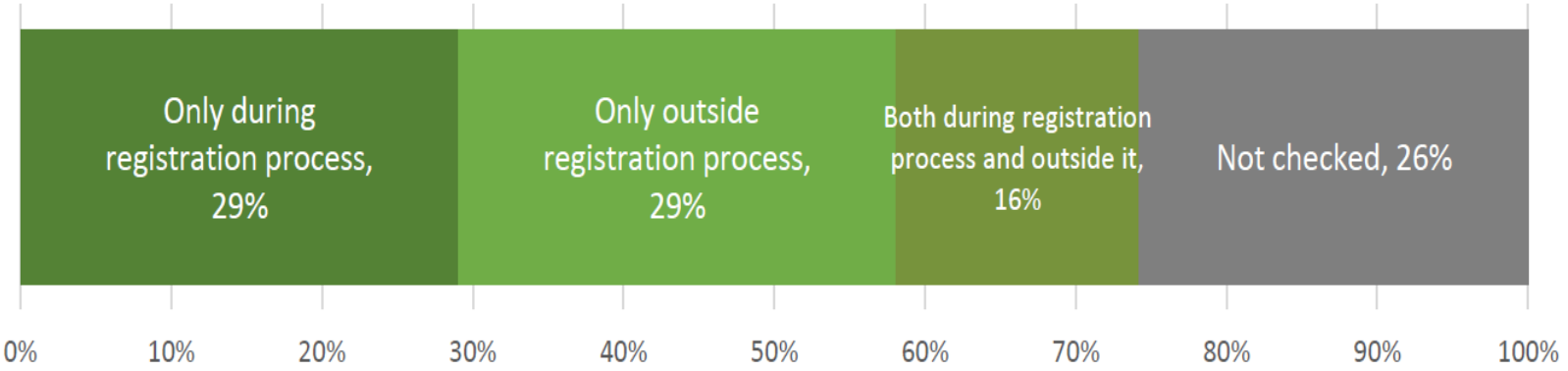
w> Host doesn't reply to ICMP requests (firewall?)
=> dns1.ssi.gouv.fr./213.56.166.96
=> dns1.certa.ssi.gouv.fr./213.56.176.3

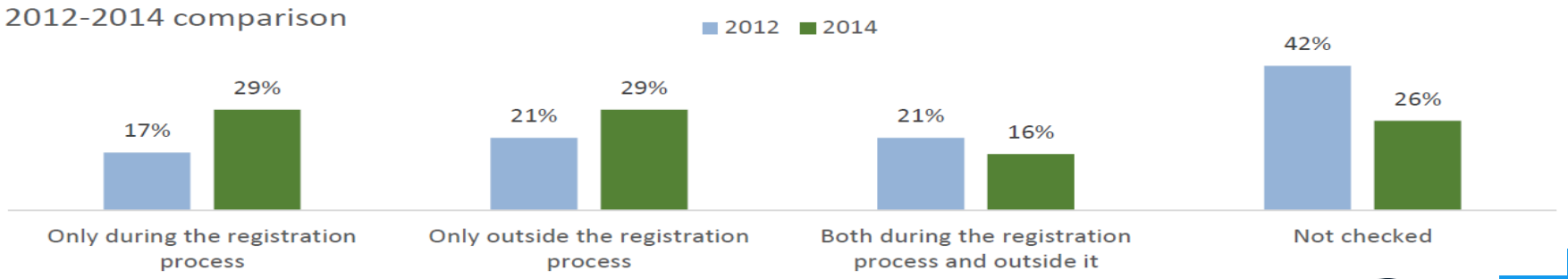
w> Can't find reverse for the nameserver IP address
=> dns1.ssi.gouv.fr./213.56.166.96
~~~~ |    fatal    || ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
f> Server doesn't listen/answer on port 53 for TCP protocol
 | Ref: IETF RFC1035 (p.32 4.2. Transport)
 |   The DNS assumes that messages will be transmitted as datagrams or in
 | a byte stream carried by a virtual circuit. While virtual circuits can
 | be used for any DNS activity, datagrams are preferred for queries due
 | to their lower overhead and better performance.
 `----- -- -- - -  -
=> dns1.certa.ssi.gouv.fr./213.56.176.3

==> FAILURE (and 4 warning(s))
```

Target Market

- ✓ End-user
- ✓ Domain administrators
- ✓ Registries
- ✓ Registrars etc..





Zonemaster



Why a new tool?

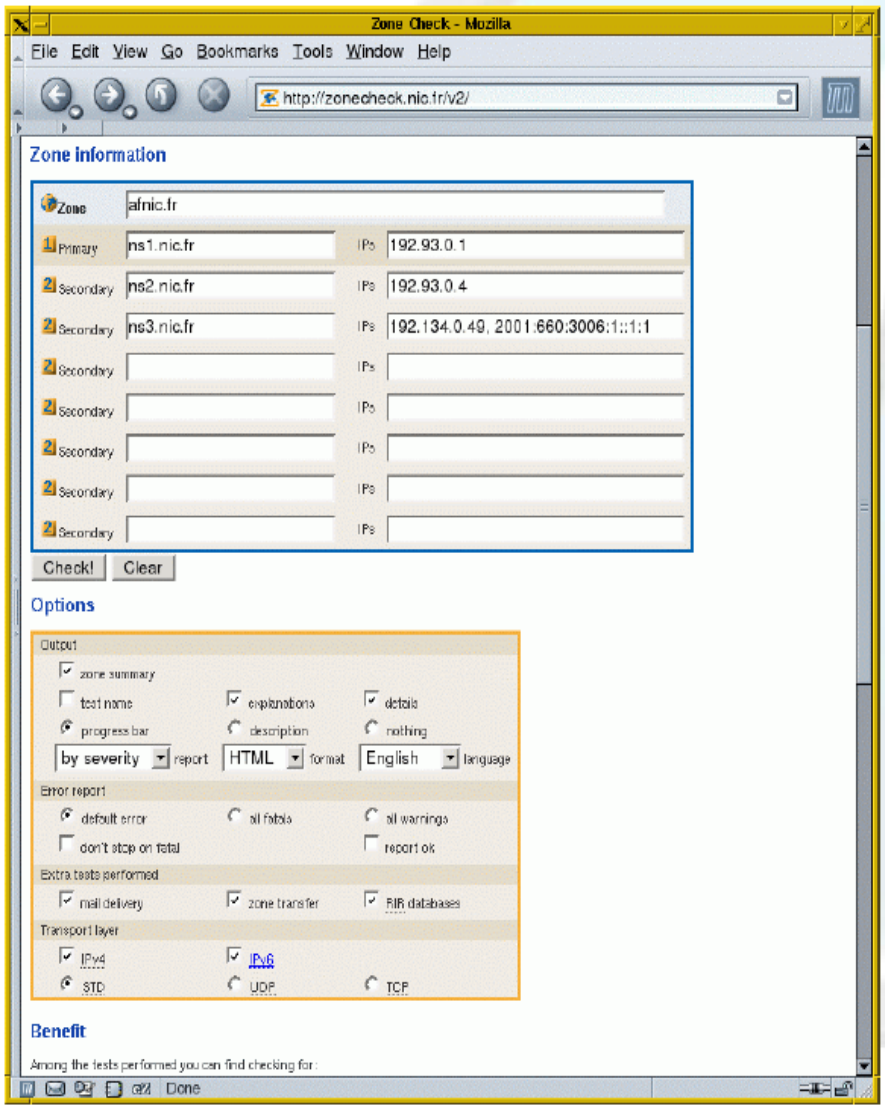
✓ Scored the existing tool (ZoneCheck and DNScheck) on the following high level criterias

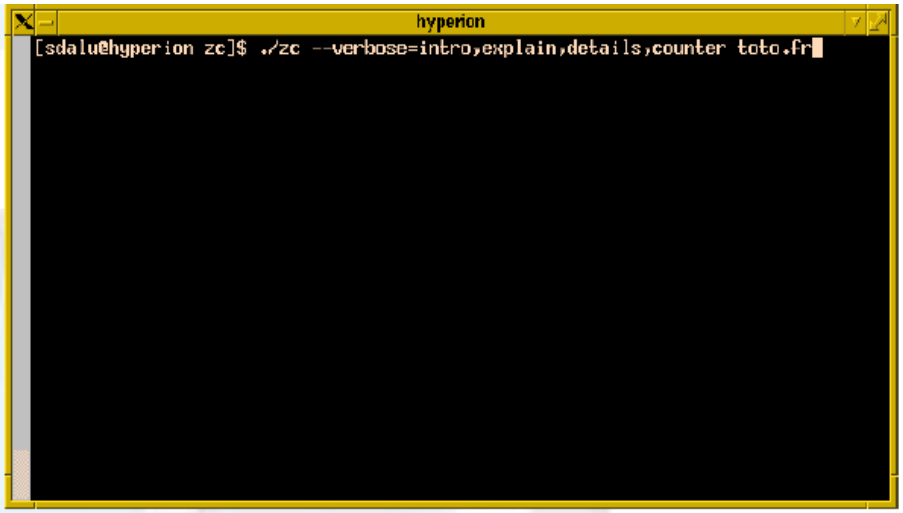
- ✓ Modularity
- ✓ Extensibility
- ✓ Optimization of network resources
- ✓ Optimization of system resources
- ✓ I/O interfaces
- ✓ Runtime behavior selection

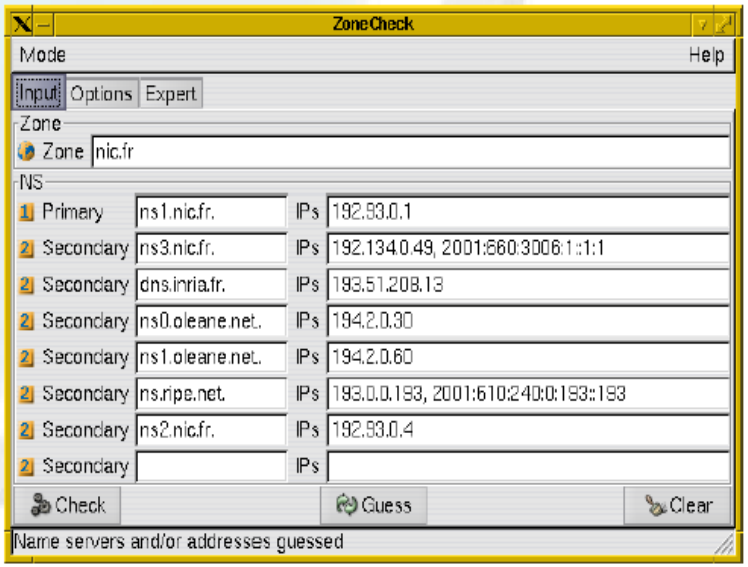
✓ Final decision to develop a tool from scratch


Benchmark

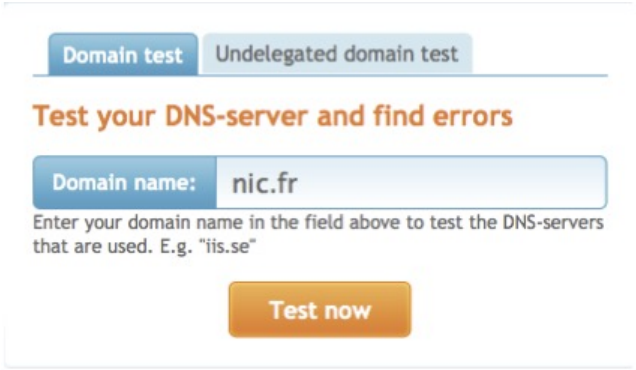
Interfaces - ZoneCheck







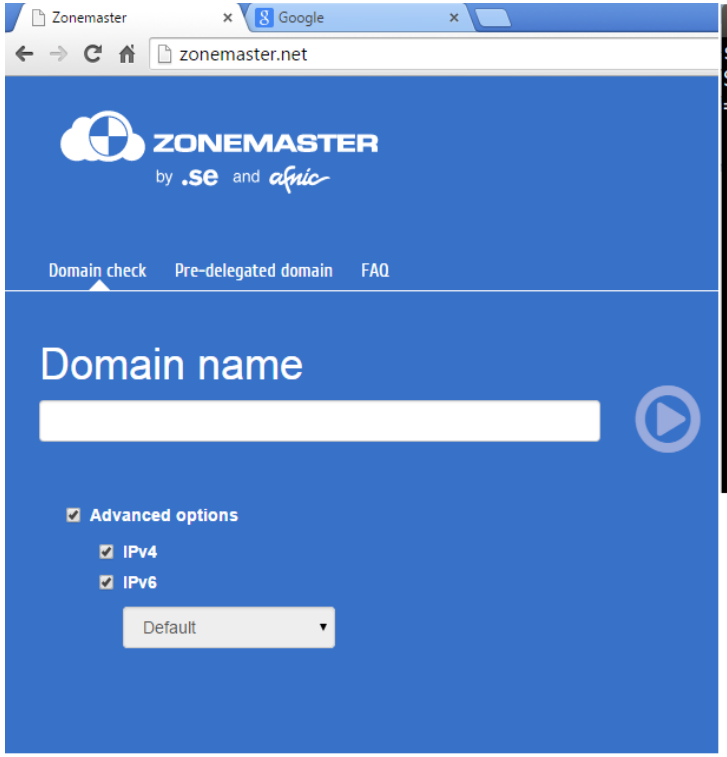
Interfaces - DNScheck

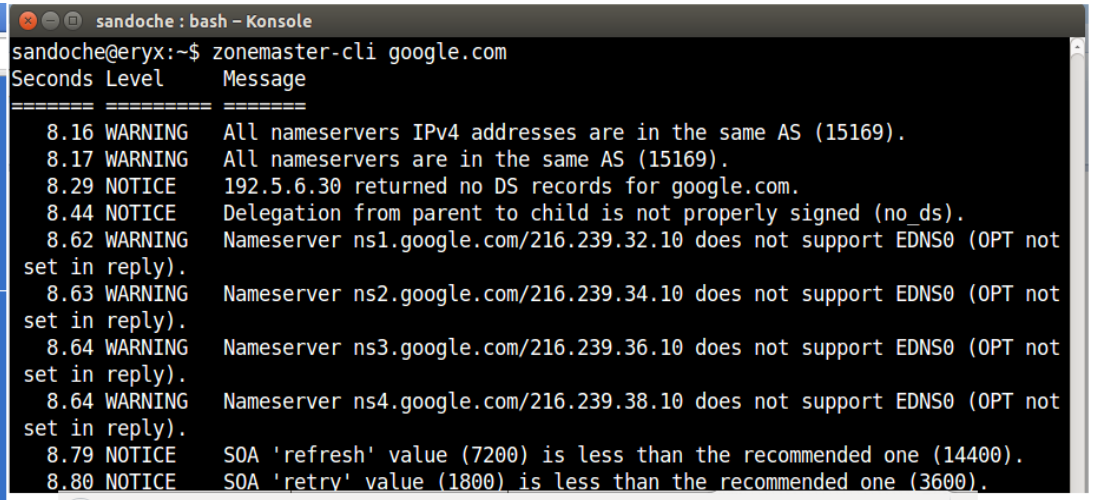


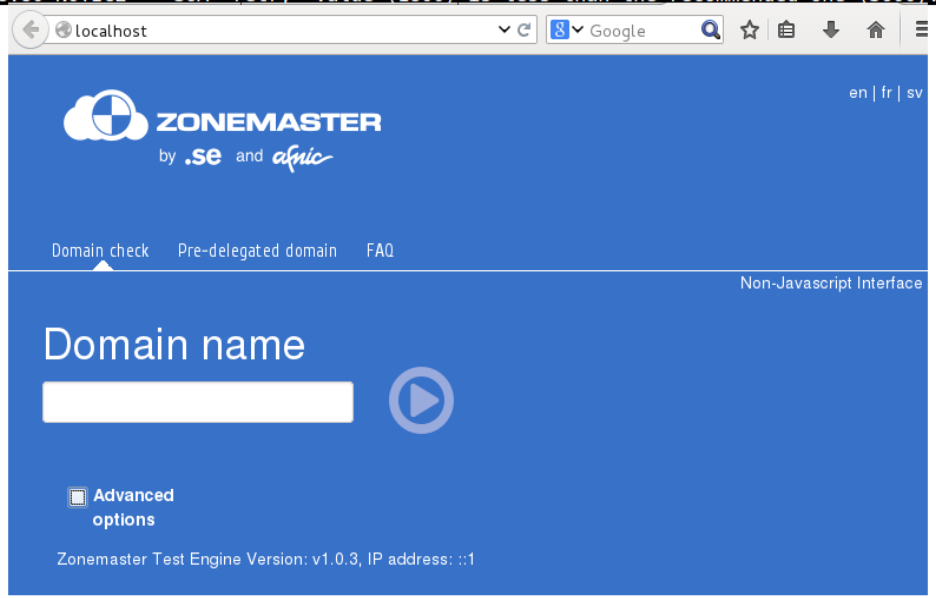

```
[rayceem@lynx ~]$ dnscheck --raw nic.fr
  0.000: nic.fr INFO [ZONE:BEGIN] nic.fr;1.6.2
  0.003: nic.fr INFO [DELEGATION:BEGIN] nic.fr
  4.141: nic.fr INFO [DELEGATION:NS_AT_PARENT] ns1.ext.nic.fr,ns1.nic.fr,ns2.nic.fr,ns3.nic.fr,ns4.ext.nic.fr,ns6.ext.nic.fr
  8.557: nic.fr INFO [DELEGATION:NS_AT_CHILD] ns1.ext.nic.fr,ns1.nic.fr,ns2.nic.fr,ns3.nic.fr,ns4.ext.nic.fr,ns6.ext.nic.fr
  8.786: nic.fr INFO [DELEGATION:GLUE_FOUND_AT_PARENT] nic.fr;ns1.ext.nic.fr;193.51.208.13
  8.983: nic.fr INFO [DELEGATION:GLUE_FOUND_AT_PARENT] nic.fr;ns1.nic.fr;192.134.4.1
  9.060: nic.fr INFO [DELEGATION:GLUE_FOUND_AT_PARENT] nic.fr;ns1.nic.fr;2001:660:3003:2:0:0:4:1
  9.159: nic.fr INFO [DELEGATION:GLUE_FOUND_AT_PARENT] nic.fr;ns2.nic.fr;192.93.0.4
  9.270: nic.fr INFO [DELEGATION:GLUE_FOUND_AT_PARENT] nic.fr;ns2.nic.fr;2001:660:3005:1:0:0:1:2
^C
```



Interfaces - Zonemaster







Batch processing

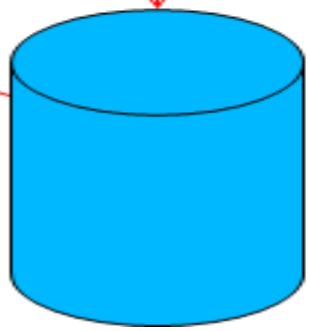




1

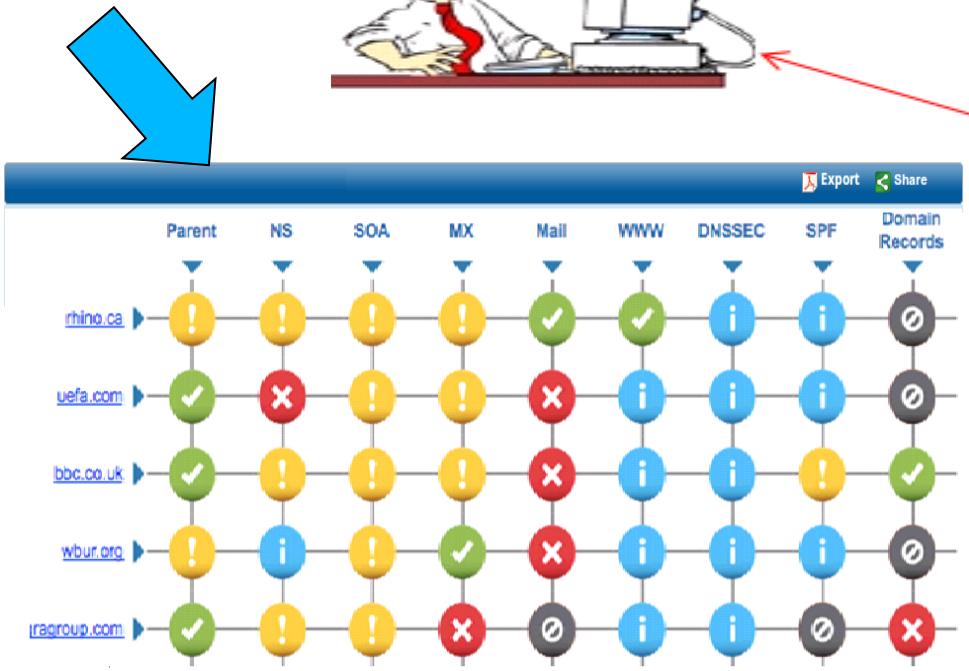


2

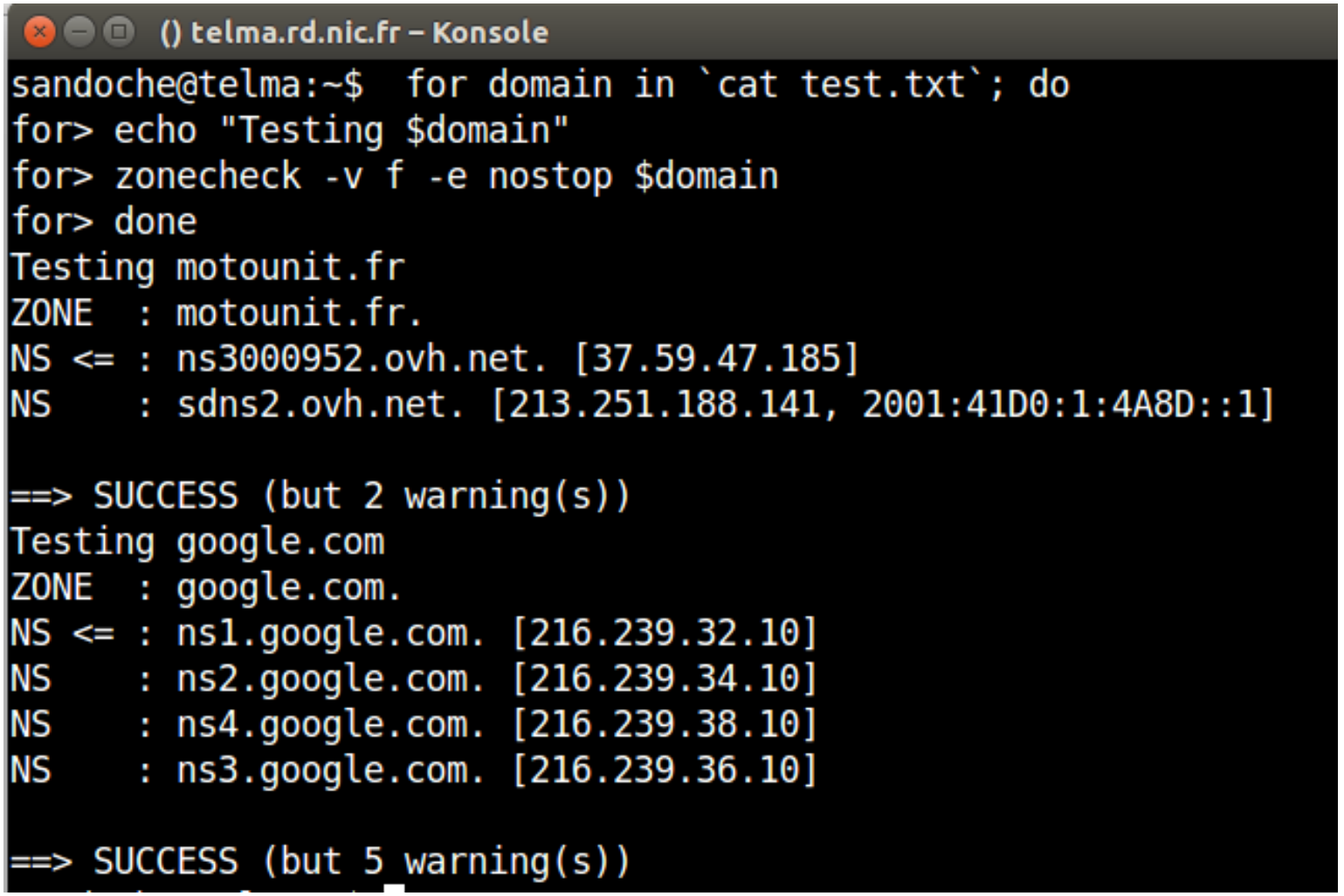


3

Target Output

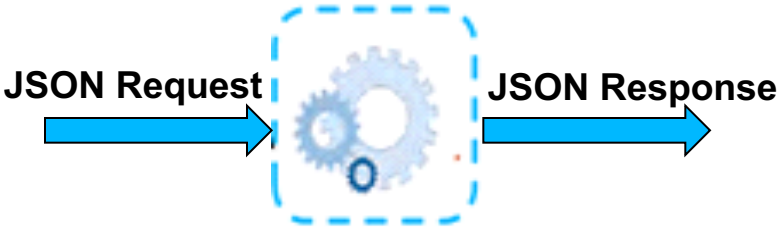


Batch mode - ZoneCheck



Batch mode - DNScheck

Batch mode – Zonemaster (ongoing work)



Easy for post processing and to obtain the target output



Documentation (1/2)

- ✓ Limited documentation in Zonecheck and DNScheck
  - ✓ Has test requirements documentation
  - ✓ Architecture
  - ✓ How the tool works?
- ✓ Zonemaster
  - ✓ Started with clear objective to document almost everything
  - ✓ All test specifications are documented
  - ✓ Anyone can use it (CC 4.0 license)
  - ✓ https://github.com/dotse/zonemaster/tree/master/docs
  - ✓ Test Requirements Task Force (CENTR)

Documentation (2/2)

BASIC00: Domain name must be valid

Test case identifier

BASIC00 Domain name must be valid

Objective

In order to begin testing the domain name from the input must be a valid domain name. The domain name must follow the rules defined in section 2.3.1 of RFC 1123. The objective of this test is to see if it is possible to have the domain name mapped into a DNS packet in order to proceed with further testing.

Inputs

The label of the domain name to be tested.

Extensible/Modular - ZoneCheck

- ✓ Test
  - ✓ Select the test family : generic, nameserver, address, extra
  - ✓ Write the corresponding test
- ✓ Configuration file
- ✓ Results such as error messages, explanation, details are translate to your locale

Extensible/Modular - DNScheck

- ✓ Test ?
- ✓Configuration file ?
- ✓ Results ?

Extensible/Modular - Zonemaster

- ✓ Test
  - ✓ Adding a test “zonemaster::Test::Example”
- ✓ Configuration file
  - ✓ Easily load the configuration/policy files
- ✓ Results
  - ✓ Developers of ZM tests should produce log messages with message tags so that it can be easily translated to human languages
  - ✓ Able to easily integrate a translation file

Network performance – From the CLI

- ✓ Small zone (motounit.fr)
  - ✓ ZoneCheck - *16.145 Seconds*
  - ✓ DNScheck - *24.127 seconds*
  - ✓ Zonemaster - *7.65 seconds*
- ✓Big zone (ibm.com)
  - ✓ ZoneCheck - *26.087 Seconds*
  - ✓ DNScheck - *67.760 seconds*
  - ✓ Zonemaster - *13.86 seconds*

CPU usage – From the CLI

```
02:02:24 PM       PID    %usr %system  %guest    %CPU   CPU  Command
02:02:26 PM     26076   13.43    1.00    0.00   14.43     1  zonecheck

02:02:26 PM       PID    %usr %system  %guest    %CPU   CPU  Command
02:02:28 PM     26076   58.00    0.50    0.00   58.50     2  zonecheck

02:02:28 PM       PID    %usr %system  %guest    %CPU   CPU  Command

02:02:30 PM       PID    %usr %system  %guest    %CPU   CPU  Command
02:02:32 PM     26076   11.00    1.50    0.00   12.50     0  zonecheck
```

```
01:57:01 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:57:03 PM  1000     23671   20.50    0.50    0.00   21.00     3  perl

01:57:03 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:57:05 PM  1000     23671   30.00    1.00    0.00   31.00     3  perl

01:57:05 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:57:07 PM  1000     23671   19.50    0.00    0.00   19.50     3  perl

01:57:07 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:57:09 PM  1000     23671   18.50    1.00    0.00   19.50     3  perl
```

CPU usage – From the CLI

```
01:58:07 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:09 PM  1000     23687   13.50    0.50    0.00   14.00     3  dnscheck

01:58:09 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:11 PM  1000     23687   12.00    0.50    0.00   12.50     3  dnscheck

01:58:11 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:13 PM  1000     23687   13.00    0.00    0.00   13.00     3  dnscheck

01:58:13 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:15 PM  1000     23687   13.50    0.00    0.00   13.50     3  dnscheck

01:58:15 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:17 PM  1000     23687   19.50    1.00    0.00   20.50     3  dnscheck

01:58:17 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:19 PM  1000     23687   13.50    0.00    0.00   13.50     3  dnscheck

01:58:19 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command

01:58:21 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command

01:58:23 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:25 PM  1000     23687    6.50    0.50    0.00    7.00     3  dnscheck

01:58:25 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:27 PM  1000     23687    4.00    0.00    0.00    4.00     3  dnscheck

01:58:27 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command

01:58:29 PM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
01:58:31 PM  1000     23687    0.50    0.00    0.00    0.50     1  dnscheck
```

Features

Feature	Zonecheck	DNScheck	Zonemaster
Time stamp on the tests being run	No	Yes	yes
Modules reporting tests as they are run	yes	yes	yes
Possibility of using non default configuration	yes	yes	yes
Different levels of verbosity	yes	yes	yes
Un delegated test	yes	yes	yes
Specifying secure delegation parameters	yes	no	yes
Possibility to specify what test(s) to run	yes	yes	yes
Ability to disable protocols at runtime	yes	No	no
Possibility to output only a summary for the results	yes	No	yes
Output a list of the tests we can run	yes	No	yes
Output the current configuration	No	No	No
Support for choice of language or locale	yes	yes	yes