Dmap: Automating Domain Name Ecosystem Measurements and Applications

Maarten Wullink, Giovane C. M. Moura, and Cristian Hesselman
SIDN Labs
Arnhem, the Netherlands
giovane.moura@sidn.nl
giovane.moura@tudelft.nl

MAPRG @ IETF102
June 19th, 2018
Montreal, Canada
The situation

Question: how to measure all these properties with current measurement tools?

Registration
- Registrant
- Registrar
- Registry

DNS Infra.
- Provider
- Auth.DNS servers

Services
- HTTP
  - Hosting Provider
  - Network
  - Contents
- SMTP
  - Email provider
  - Network
  - StartTLS
- TLS (HTTP)
  - Certificate
  - CA
- Others
The situation

- **Answer:** `zmap + dig + masscan + ... + ad gustum`

you can do it, but it ain’t pretty...
The situation

The problem:
1. *wasted time* spent on repetitive tasks
2. *heterogeneous data formats* per tool
3. more complexity $\rightarrow$ more errors
4. hard to reproduce studies
Can we do better than this?

We decided to build a new tool: **Dmap**

- **Dmap**: Domain name ecosystem mapper
- It **automates** measurements of 5 protocols (HTTP, HTTPs, DNS, TLS, SMTP) and screenshot
- Produces a unified data model (SQL interface)

We open it for researchers:

- [https://dmap.sidnlabs.nl](https://dmap.sidnlabs.nl)
- Paper presented at TMA 2018
Applications

Profiling Alexa 1 million

- **Try it**! dataset and SQL code available at https://dmap.sidnlabs.nl
- Each result here obtained with SQL
- Hypothesis tests within seconds
Applications: Alexa profiling

77% support HTTPS, 1 in 5 are Let’s Encrypt

<table>
<thead>
<tr>
<th>DNS</th>
<th>IPv4</th>
<th>IPv6</th>
<th>IPv6/IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td># Domains (OK)</td>
<td>972,155</td>
<td>153,485</td>
<td>0.16</td>
</tr>
<tr>
<td># Unique NSes</td>
<td>289,014</td>
<td>26,127</td>
<td>0.09</td>
</tr>
<tr>
<td># Unique IP</td>
<td>210,650</td>
<td>19,754</td>
<td>0.09</td>
</tr>
<tr>
<td># Unique ASes</td>
<td>18,418</td>
<td>3,178</td>
<td>0.17</td>
</tr>
<tr>
<td># CDN Cloudflare</td>
<td>117,538</td>
<td>115,396</td>
<td>0.98</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTP</th>
<th>IPv4</th>
<th>IPv6</th>
<th>IPv6/IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td># Domains (OK)</td>
<td>968,338</td>
<td>153,485</td>
<td>0.16</td>
</tr>
<tr>
<td># HTML 5</td>
<td>681,757</td>
<td>116,066</td>
<td>0.17</td>
</tr>
<tr>
<td>Bytes (median)</td>
<td>53,889</td>
<td>64,735</td>
<td>1.20</td>
</tr>
<tr>
<td>External links (median)</td>
<td>7</td>
<td>8</td>
<td>1.14</td>
</tr>
<tr>
<td>Internal links (median)</td>
<td>67</td>
<td>75</td>
<td>1.12</td>
</tr>
<tr>
<td>Cookies (median)</td>
<td>1</td>
<td>1</td>
<td>1.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TLS</th>
<th>IPv4</th>
<th>IPv6</th>
<th>IPv6/IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td># Domains (OK)</td>
<td>772,455</td>
<td>129,443</td>
<td>0.17</td>
</tr>
<tr>
<td># Let's Encrypt</td>
<td>165,526</td>
<td>10,466</td>
<td>0.06</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SMTP</th>
<th>IPv4</th>
<th>IPv6</th>
<th>IPv6/IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td># Domains (OK)</td>
<td>843,126</td>
<td>190,736</td>
<td>0.23</td>
</tr>
<tr>
<td># Unique SMTP</td>
<td>501,848</td>
<td>24,311</td>
<td>0.05</td>
</tr>
<tr>
<td># Unique IP</td>
<td>286,504</td>
<td>10,113</td>
<td>0.04</td>
</tr>
<tr>
<td># Unique StartTLS</td>
<td>302,871</td>
<td>8,016</td>
<td>0.03</td>
</tr>
</tbody>
</table>
Questions?

Download it!

- [https://dmap.sidnlabs.nl](https://dmap.sidnlabs.nl)
- **contact**: giovane.moura@sidn.nl
- Paper at [https://dmap.sidnlabs.nl/paper.pdf](https://dmap.sidnlabs.nl/paper.pdf)