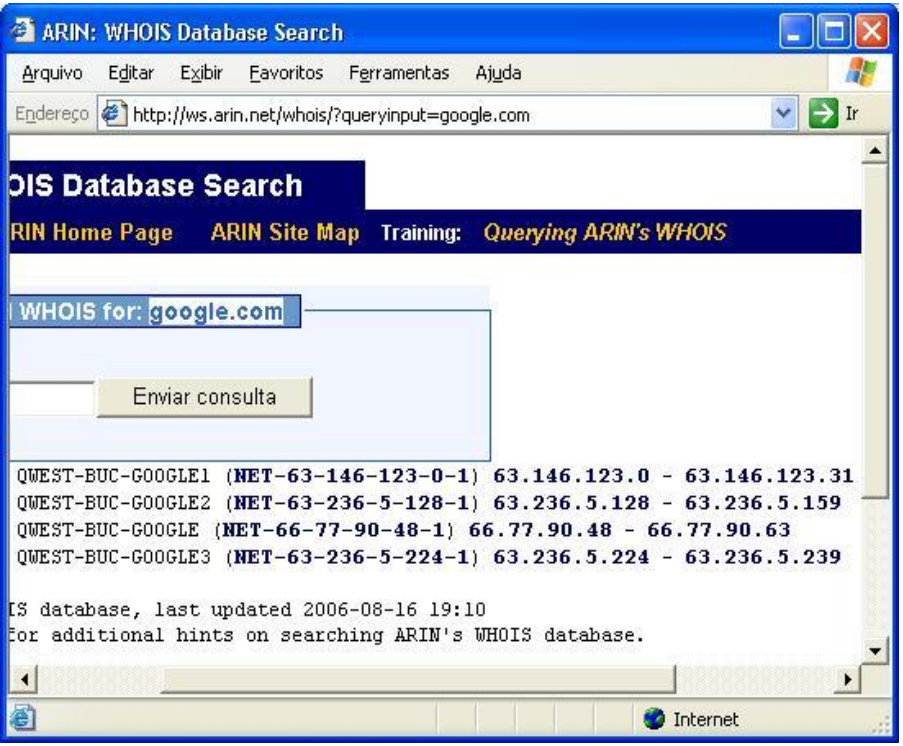
Enumeração

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking



Pesquisa inicial
(FootPrinting)

- Pesquisa geral
- Ping e traceroute
- Sites de emprego
- Whois (internic e arin)
- DNS Zone Transfer
- Google
- Archive.Org
- Mail Tracking

Ping e traceroute

```
C:\>ping -a www.defhack.com.br

Disparando defhack.com.br [212.1.215.218] com 32 bytes de dados:
Resposta de 212.1.215.218: bytes=32 tempo=314ms TTL=48

Estatísticas do Ping para 212.1.215.218:
    Pacotes: Enviados = 1, Recebidos = 1, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 314ms, Máximo = 314ms, Média = 314ms
```

- Permitem descobrir informações como:
  - IP e nome de **servidores** e **roteadores** intermediários
  - Se há **bloqueio** de firewalls filtro de pacote

Sobre a vaga

Salário

- R$ 1.200,00 a R$ 2.000,00 (Bruto mensal)

Descrição

- Área e especialização profissional: Informática, TI,
- Nível hierárquico: Analista
- Número de vagas: 2
- Local de trabalho: Belo Horizonte, MG
- Regime de contratação de tipo Efetivo - CLT
- Jornada Período Integral
- Suporte a:
- Windows Active Directory
- Virtualizacao VMware vSphere (basico)
- Windows XP \ 7
- Office 2010 \ 2013

Pesquisando sites de emprego

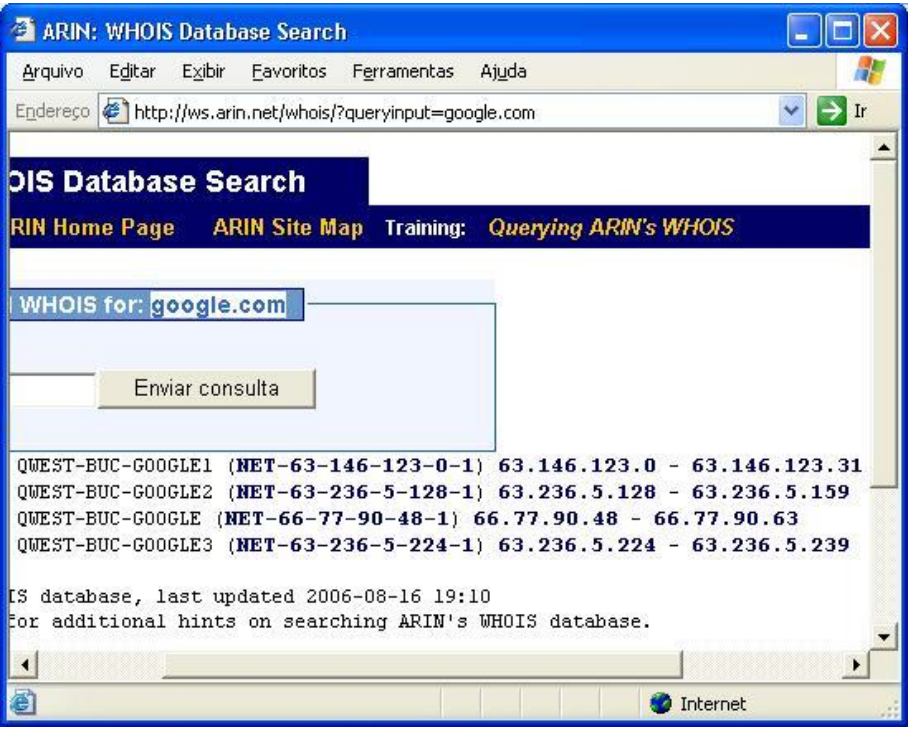
Vagas de emprego frequentemente revelam mais do que deveriam sobre a estrutura de TI de uma empresa

```
domínio:        planalto.gov.br
titular:        PRESIDENCIA DA REPUBLICA
documento:      000.394.411/0001-09
responsável:    Secretaria de Administração
endereço:       PÇA DOS TRES PODERES, 109,
endereço:       70150-900 - Brasília - DF
país:           BR
telefone:       (61) 34112159 []
c-titular:      MAR79
c-admin:        MAR79
```

Whois

Pesquisando domínios

- Permite descobrir informações sobre um domínio
- Vários sites podem ser usados.
- Exemplo: *registro.br* e *internic.net*



Whois

Pesquisando IPs

- ARIN.NET
- Permite descobrir o range de endereços IP de uma rede pública

DNS Zone Transfer

```
187-60-128-94                           A       187.60.128.94
187-60-134-99                           A       187.60.134.99
187-60-130-95                           A       187.60.130.95
187-60-128-95                           A       187.60.128.95
187-60-130-96                           A       187.60.130.96
187-60-128-96                           A       187.60.128.96
187-60-130-97                           A       187.60.130.97
187-60-128-97                           A       187.60.128.97
187-60-130-98                           A       187.60.130.98
187-60-128-98                           A       187.60.128.98
187-60-130-99                           A       187.60.130.99
```

- Transfere zonas de servidores DNS secundários vulneráveis
- Pode usar o dig ou o nslookup
- Exemplo (nslookup):

```
server ns2.empresa.com
set type=ANY
ls -d empresa.com
```

Google Hacking

- Descobrir informações pelo google usando comandos como:
  site, **filetype**, **inurl** e **index of**, entre outros.

site:products.sel.sony.com perl

5 results (0.16 seconds) Go to Go

Sony - Open Source Code - English - dash™
9 Feb 2011 ... **perl**. **perl**-5.10.0.tar.gz · GPL v2. ssh sshd. openssh-5.1p1.tar.gz · BSD License. libtiff. tiff-3.8.2.tar.gz · Libtiff License ...
products.sel.sony.com/opensource/source_dash.shtml - Cached - Similar

get_datasheet.cgi - Sony USA
usr/local/bin/**perl** eval { ##
Read in the string from the form ...
products.sel.sony.com/cgi-bin/semi/get_datasheet.cgi - Cached

wishlist - Sony - [Translate this page]
usr/bin/**perl** umask(02); use CGI; # Setting Security for the script $CGI::POST_MAX=1024 * 100; # max 100K posts $CGI::DISABLE_UPLOADS = 1; ...
products.sel.sony.com/cgi-bin/wishlist - Cached

Sony - Open Source Code - Spanish - dash™ - [Translate this page]

Archive.Org – WayBack Machine

- Permite visualizar versões passadas de qualquer website já criado desde o surgimento da WEB.
- Extremamente útil para ver a evolução de uma empresa
- Mostra o “ano” de quando o site foi criado. Isso é muito relevante pois podemos saber quando a empresa começou a atuar.
- Outra vantagem: poder “rever” o conteúdo de um site que já saiu do ar.

Archive.Org – WayBack Machine

INTERNET ARCHIVE
WayBackMachine

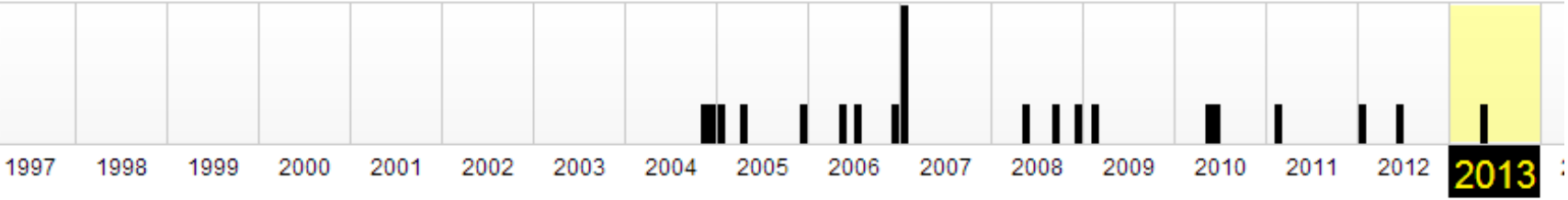
http://www.defhack.com

BROWSE HISTORY

http://www.defhack.com

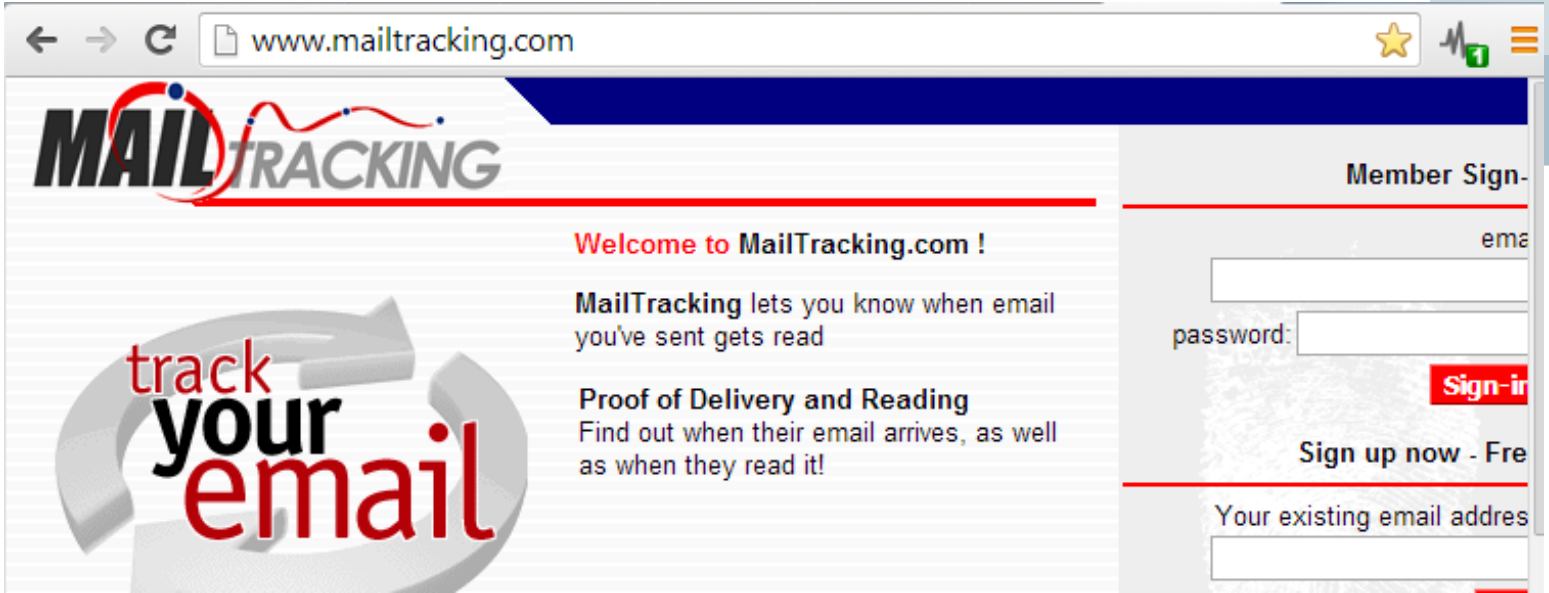
Saved **22 times** between Novembro 14, 2004 and Maio 29, 2013.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



Mail Tracking

- **Mail Tracking** é um serviço extremamente útil, que permite monitorar os e-mails que você envia para saber se o destinatário leu a mensagem, o horário que isto aconteceu – e o mais importante – o endereço IP do sistema que destinatário estava utilizando no momento.



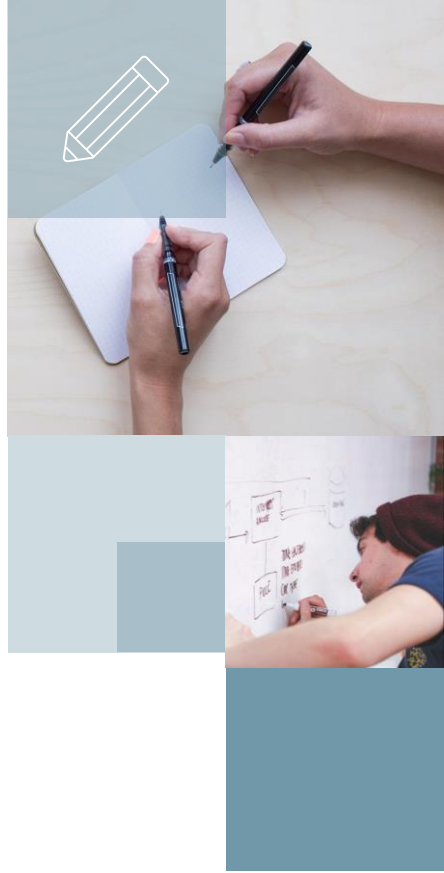
Mail Tracking

- Basta se cadastrar no site e mandar o seu e-mail com “mailtracking.com” no final da mensagem. Exemplo: fulano@empresa.com.br.mailtracking.com .
- Assim que o destinatário abrir a mensagem, logue no mailtracking e veja os dados capturados:

Opened	
Opened	2014/03/08 , 18:38:57pm (UTC -3:00) - 19sec after sending
Location	Sao Paulo, Brazil (86% likelihood)
Opened on	c911dcfd.virtua.com.br (201.17.220.253:55650
Language	of recipient's PC: pt-BR (Portuguese/Brazil), pt;q=0.8 (Portugues
Browser	used by recipient: Moz/5.0 (WinNT 6.1; WOW64) AppleWebKit/5:
Accepts	Files browser can open: i/webp,*/*;q=0.8
Last log	No more activity after 2014/03/08 , 18:40:52pm (UTC -3:00) - I

Facebook Tracking
Blasze

- O site Blasze.tk permite gerar um link que pode ser colado na timeline do Facebook, na janela de chat (ou em qualquer outra rede social), que redirecionará o usuário para um site e capturará seu endereço IP e informações básicas de user-agent.
- Recomenda-se usar um encurtador de URL como goo.gl.



Share This Link
http://blasze.tk/HXIU5C

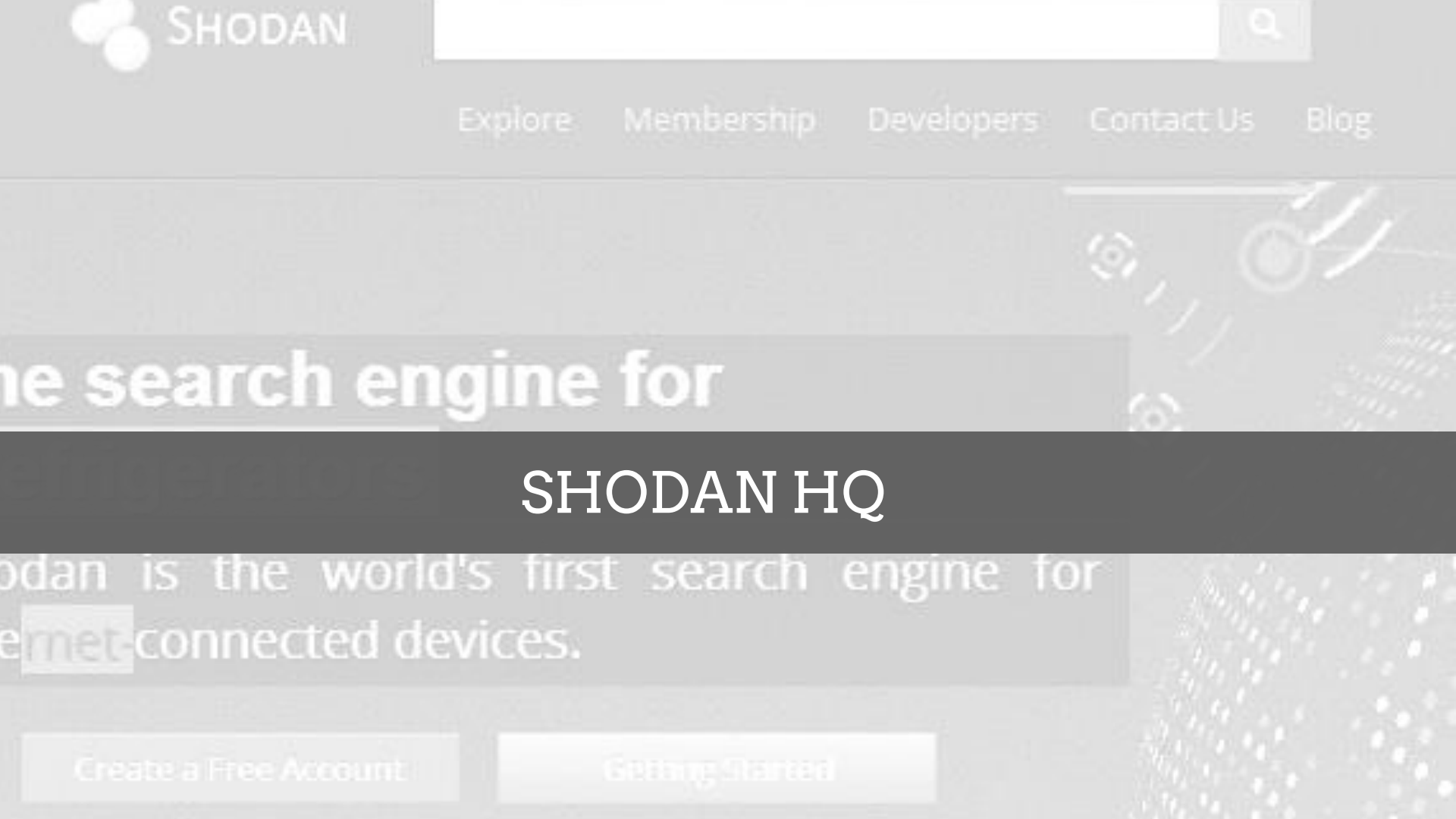
Blasze IP Logger

Link Information

ACCESS CODE	PS9TXL
CREATED DATE	2015-6-29 16:1:10
ORIGINAL URL	http://www.tecmundo.com.br
TRACKING LINK (GIVE THIS OUT)	http://blasze.tk/HXIU5C

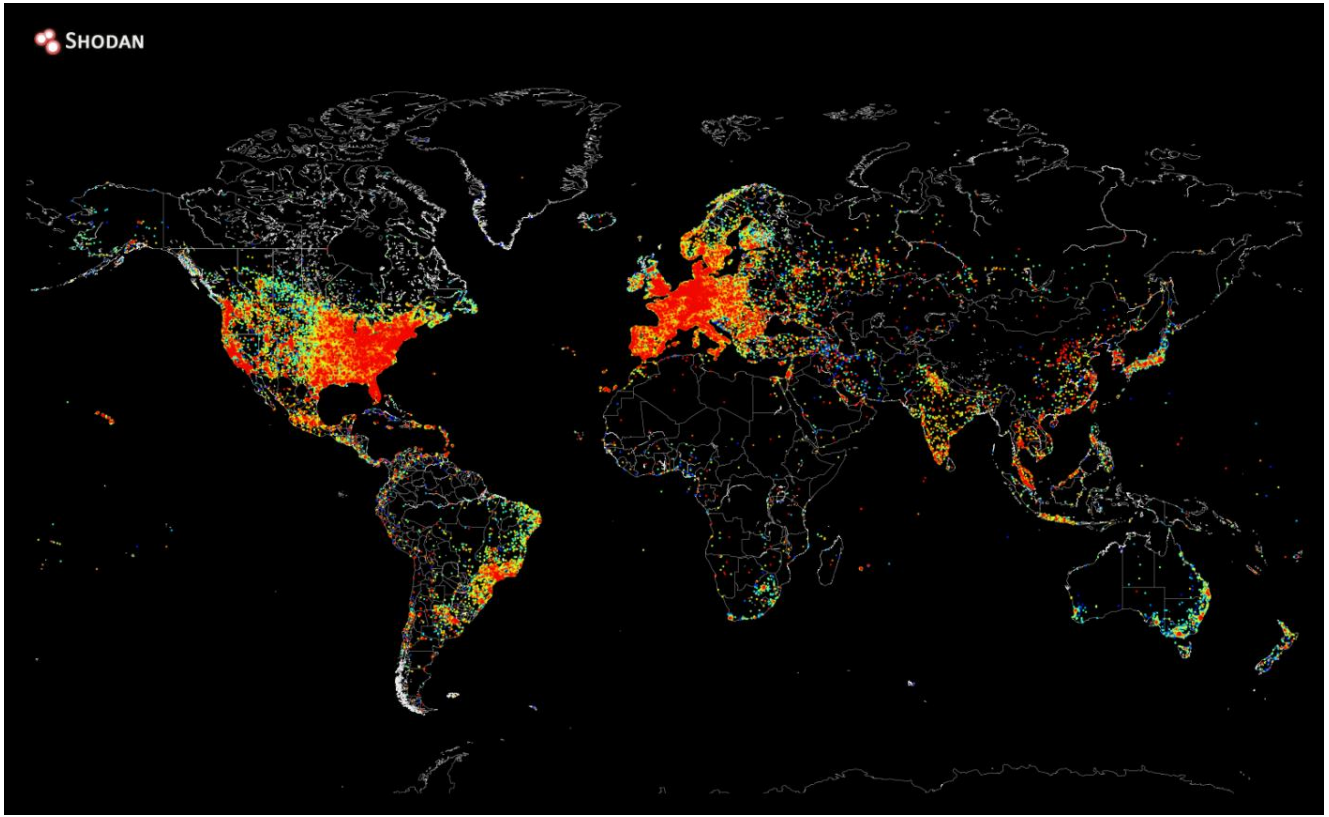
Access Logs

DATE	IP ADDRESS	USER AGENT	HOSTNAME	REFERRING URL
2015-6-29 16:2:13	191.185.38.36,66.249.85.241	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko; Google Web Preview) Chrome/27.0.1453 Safari/537.36		http://www.google.com/search
2015-6-29 16:2:32	173.252.100.116	facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)		


SHODAN
Explore
Membership
Developers
Contact Us
Blog
ne search engine for
odan is the world's first search engine for
e net-connected devices.
Create a Free Account
Getting Started

SHODAN HQ

Mapa de dispositivos mundial



Termos de pesquisa

Entre os comandos que podemos utilizar para uma pesquisa, estão:

- **country:** país
- **city:** cidade
- **Port:** porta
- **geo:** coordenadas Geográficas
- **net:** Sub-rede
- **os:** Sistema operacional
- **hostname:** Nome de host
- **before:** Antes
- **After:** depois

A sintaxe usada é: `comando:argumento`

SHODAN

country:BR

Explore Membership Developers Contact Us Blog

Exploits Maps Download Results

TOP COUNTRIES

Brazil	26,5...

TOP CITIES

Rio De Janeiro	931,...
Curitiba	580,...
Salvador	483,...
Belo Horizonte	377,...
Recife	358,...

TOP SERVICES

SNMP	5,54...
UPnP	4,95...
HTTP	4,74...
Telnet	3,12...
SSH	1,89...

TOP ORGANIZATIONS

Global Villag...	6,75...
Oi Velox	4,19...

Showing results 1 - 10 of 22,357,034

189.4.162.209
bd04a2d1.virtua.com.br
Virtua
Added on 2014-09-08 13:55:44 GMT
Brazil, Santos
Details

```
Technicolor CableHome Gateway <<HW_REV: 2.0; VENDOR: Technicolor; BOOTR:
V: STC7.05.21; MODEL: TC7110.B>>
```

186.217.116.16
Universidade Estadual Paulista
Added on 2014-09-08 13:55:40 GMT
Brazil
Details

```
220 ET0021B78403A4 Lexmark X652de FTP Server NR.APS.N528 ready.
230 User anonymous logged in.
502 HELP command not implemented.
```

404 Not Found
177.134.77.146
177.134.77.146.dynamic.adsl.gvt.net.br
Global Village Telecom
Added on 2014-09-08 13:55:40 GMT
Brazil, Porto Alegre
Details

```
HTTP/1.0 404 Not found
Connection: close
Content-type: text/html
```

PAÍS

country:BR