Como se defender utilizando software livre na era da espionagem

Breno Neves

Dia da Liberdade de Software 2013

Setembro de 2013

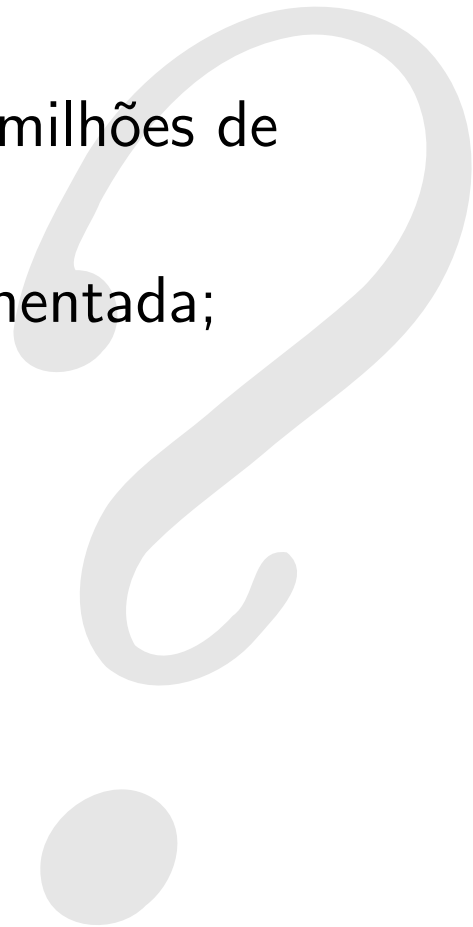
Conteúdo da apresentação

Para descontrair

- Alguém aqui conhece:
  - Carolina da Luz?
  - Ismael Rocha?
  - Caroline Mantovani?
  - Nívia Santos?

Para descontrair

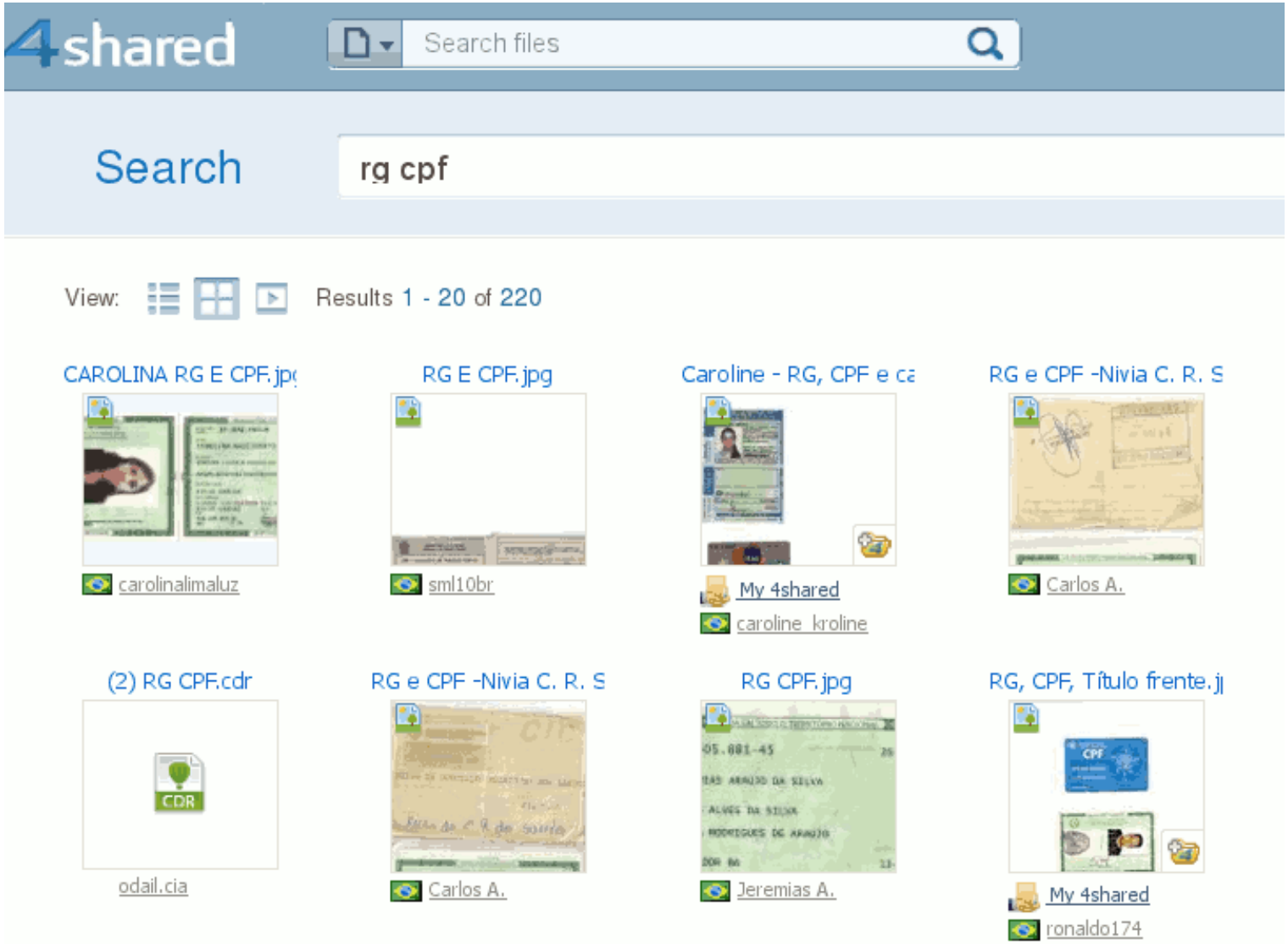
- Não possuem um canal do youtube com 50 milhões de visualizações;
- Não são donos de uma fan page ultra movimentada;
- Não administram um blog famoso;
- Não trabalham na Microsoft.
- Não estão aqui.

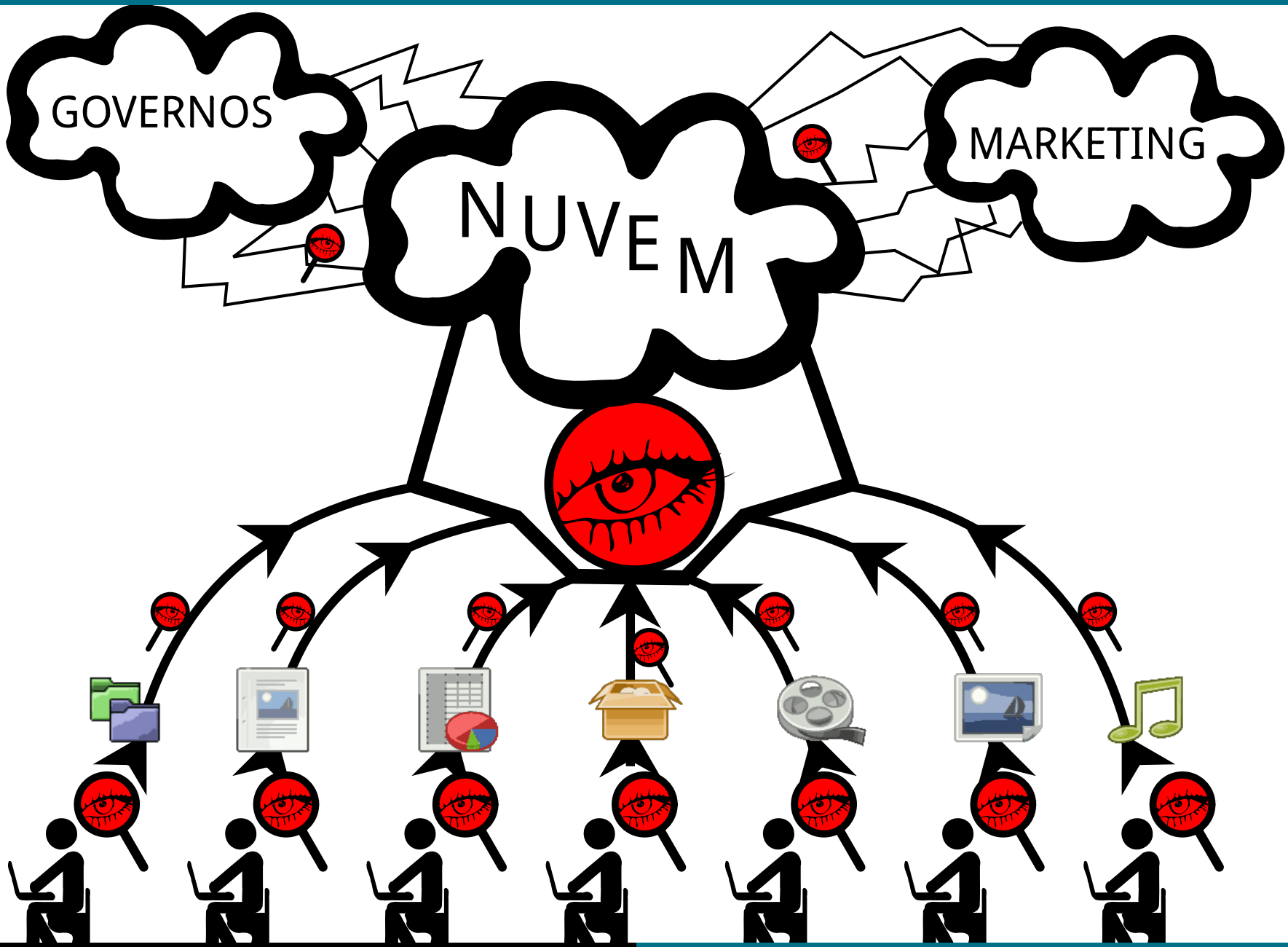


Para descontrair

Mas ficaram famosos de outra forma.

Para descontrair




GOVERNOS
NUVEM
MARKETING

Sniffers

- São softwares que capturam todo o tráfego de rede.
- Dentre os mais conhecidos estão o tcpdump e wireshark.
- Podemos utilizá-los para coletar as informações trocadas entre os softwares e computadores na Internet.
- Podemos utilizá-los para detectar uma pequena parte da espionagem que nos cerca, e entender como tais serviços funcionam.

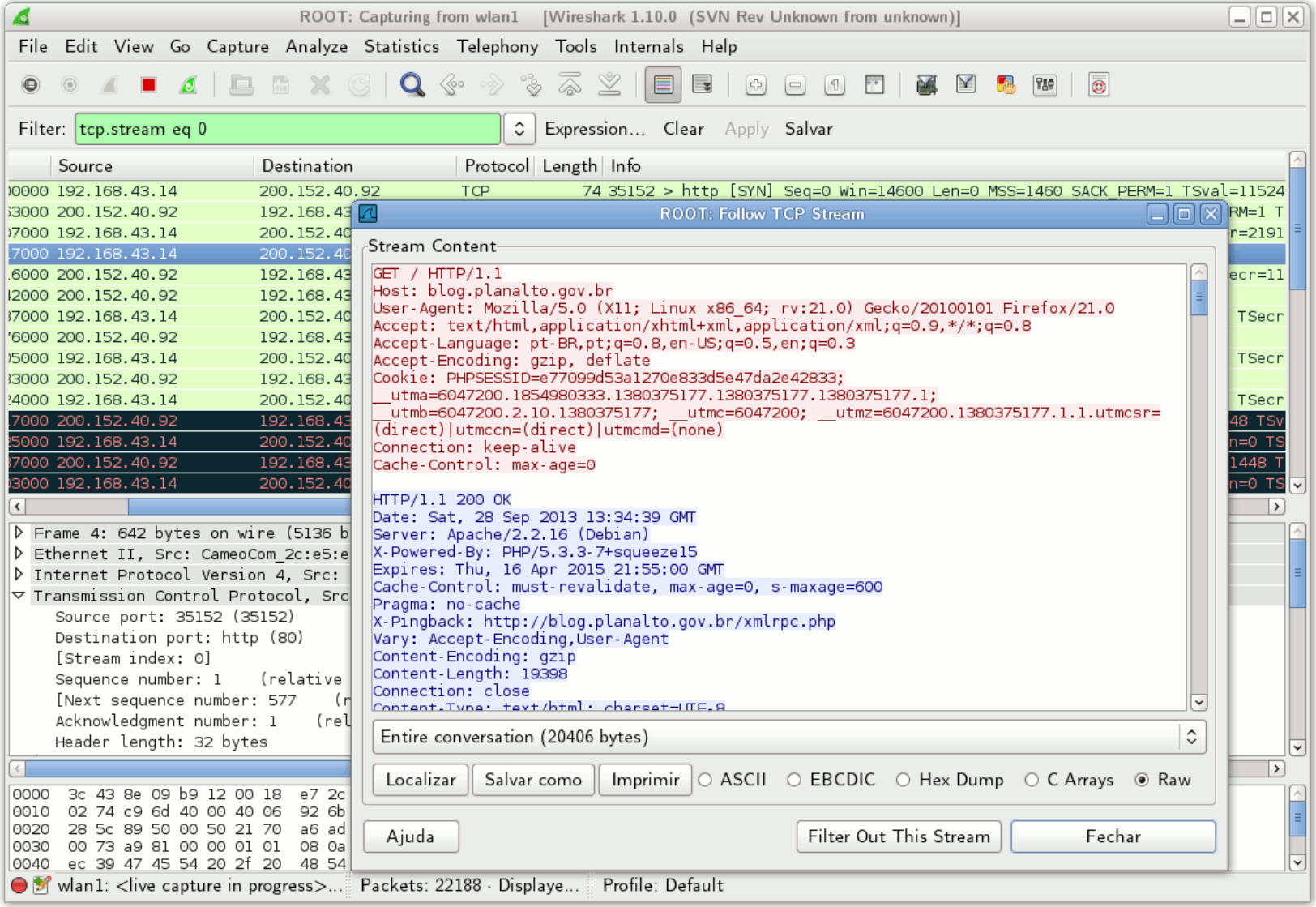
TCPDUMP/Libpcap

- TCPDUMP: Ferramenta em modo texto muito poderosa para capturar o tráfego da rede.
- A libpcap serve como base para a criação de sniffers, originalmente construída em C mas há wrappers para mais de 10 linguagens.
- Diversas ferramentas se baseiam na libpcap, como o ngrep, wireshark, snort, nmap, kismet, iftop...

Wireshark

- De acordo com o próprio software, é o analista de protocolos de rede mais popular do mundo! **E é livre**.
- Captura de praticamente qualquer dispositivo: usb, wireless, ethernet, bluetooth, local, etc.
- Possui interface bastante intuitiva;
- É capaz de interpretar diversos protocolos, pode recriar o fluxo de uma conexão TCP.

Wireshark


ROOT: Capturing from wlan1 [Wireshark 1.10.0 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 0
Expression... Clear Apply Salvar
Source Destination Protocol Length Info
ROOT: Follow TCP Stream
Stream Content
GET / HTTP/1.1
Host: blog.planalto.gov.br
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:21.0) Gecko/20100101 Firefox/21.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=e77099d53a1270e833d5e47da2e42833;
__utma=6047200.1854980333.1380375177.1380375177.1380375177.1;
__utmb=6047200.2.10.1380375177; __utmc=6047200; __utmz=6047200.1380375177.1.1.utmcsr=
(direct)|utmccn=(direct)|utmcmd=(none)
Connection: keep-alive
Cache-Control: max-age=0
HTTP/1.1 200 OK
Date: Sat, 28 Sep 2013 13:34:39 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze15
Expires: Thu, 16 Apr 2015 21:55:00 GMT
Cache-Control: must-revalidate, max-age=0, s-maxage=600
Pragma: no-cache
X-Pingback: http://blog.planalto.gov.br/xmlrpc.php
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 19398
Connection: close
Entire conversation (20406 bytes)
Localizar Salvar como Imprimir ASCII EBCDIC Hex Dump C Arrays Raw
Ajuda Filter Out This Stream Fechar
Frame 4: 642 bytes on wire (5136 b
Ethernet II, Src: CameoCom_2c:e5:e
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src
Source port: 35152 (35152)
Destination port: http (80)
[Stream index: 0]
Sequence number: 1 (relative
[Next sequence number: 577
Acknowledgment number: 1
Header length: 32 bytes
wlan1: <live capture in progress>...
Packets: 22188 · Displaye...
Profile: Default

DNS

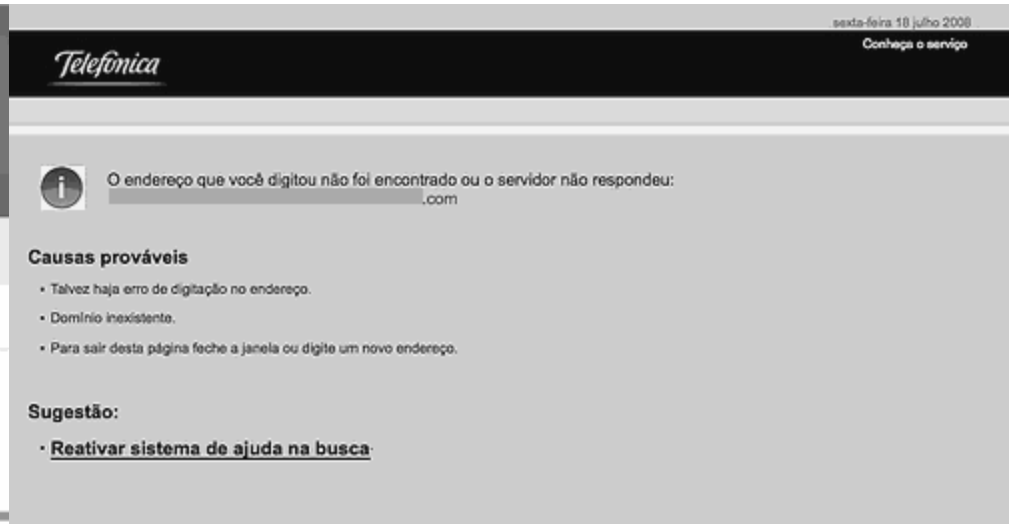
- *Domain Name System*
- Neste contexto, o protocolo DNS é utilizado para transformar um nome de domínio em um endereço IP, ou vice-versa.
- Há vários níveis hierárquicos quando ocorre a resolução de um determinado endereço:
  1. Banco de dados local (hosts)
  2. Servidor primário (resolv.conf)
  3. Servidor secundário
  4. Outros servidores, caso esteja configurado.

DNS – Sequestro

- Fica caracterizado nas seguintes situações:
  1. Se um host não existe, vem um IP padrão;
  2. O IP resolvido pelo servidor é diferente do verdadeiro;
- Tal prática tem sido feita por vários provedores.
  - Domínios inexistentes são sequestrados para uma empresa de marketing.
  - Alguns sites ou serviços muito acessados são redirecionados para servidores do provedor.


service by
YAHOO!
SEARCH MARKETING
Buscar
BrasilTelecom
O endereço que você digitou não foi encontrado:
"www.[redacted].com.br/"
WEBLINKS
SUGESTÕES


Endereço que você digitou não foi encontrado:
www.[redacted].com.br
oi
BUSCAR
Sugestões
Flores
Viagem
Compras
Informática
Decoração
Celulares
Comunicação social
Presentes
Empregos
Livros
Móveis
Eletrodomésticos


sexta-feira 18 julho 2008
Conheça o serviço
Telefônica
O endereço que você digitou não foi encontrado ou o servidor não respondeu:
[redacted].com
Causas prováveis
• Talvez haja erro de digitação no endereço.
• Domínio inexistente.
• Para sair desta página feche a janela ou digite um novo endereço.
Sugestão:
• Reativar sistema de ajuda na busca

HTTP

- *Hypertext Transfer Protocol*, ou traduzindo, protocolo de transferência de hipertexto, é a base da *World Wide Web*, e sua última definição foi em 1999 pela RFC 2616.
- É bastante simples, o navegador faz a requisição, o servidor faz uma resposta;
- Cada requisição e cada resposta possuem duas áreas: o cabeçalho e o conteúdo, separadas por duas quebras de linha.

HTTP

```
GET /vid01/ HTTP/1.1
Host: www.brenoneves.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:21.0) Gecko/20100101 Firefox/21
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Date: Sat, 21 Sep 2013 00:12:50 GMT
Server: Apache
Content-Encoding: gzip
Connection: Keep-Alive
Content-Type: text/html

<html>
<head>
...
```

HTTP

- Quando **qualquer tipo de objeto** é incluído em uma página, a requisição para este objeto terá o cabeçalho **Referer** que informa o endereço completo da página.
  - Imagens
  - Scripts
  - CSS
  - Áudio
  - Video
  - Plugins / Java / Flash
- A maioria dos navegadores aceita cookies nesta requisição, assim funcionam os produtos como "Google Analytics".

HTTP

```
GET /vid01/videos.ogg HTTP/1.1
Host: brenoneves.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:21.0) Gecko/20100101 Firefox/21
Accept: video/webm,video/ogg,video/*;q=0.9,application/ogg;q=0.7,audio/*;q=0.6
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://brenoneves.org/vid01/
Connection: keep-alive

HTTP/1.1 200 OK
Date: Sat, 21 Sep 2013 09:20:20 GMT
Server: Apache
Last-Modified: Sat, 27 Jul 2013 17:25:13 GMT
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: video/ogg
...
```

HTTP

- Requisição: **método, endereço, protocolo**;

Host	O nome do servidor;
User-Agent	O navegador;
Cookie	Cookies enviados previamente pelo servidor;
Referer	De onde veio?

- Resposta: **protocolo, código, descrição**

Date	Data no servidor;
Server	Nome do servidor;
Last-Modified	Última modificação do arquivo/página;
Content-Type	Tipo de arquivo, o mime-type;
Set-Cookie	Cookie a ser gravado no navegador.

HTTP – Rastreamento

- Na maioria dos casos, o rastreamento usando o protocolo HTTP utiliza o seguinte fluxo:
  1. A página inclui algum item de terceiros (script)
  2. Ao carregar o item, é enviado o REFERER;
  3. Na resposta há um SET-COOKIE;
  4. A partir deste momento, se o usuário entrar em qualquer outra página que tenha este mesmo item, será rastreada.
  5. Isto te lembra alguma coisa?

HTTP

```
GET /f.gif?_=1380366108173&id=twitter-widget-0&lang=pt&screen_name=ComUbuntu
      Brasil&show_count=true&show_screen_name=false&size=m&twttr_variant=2.0&
      twttr_referrer=http%3A%2F%2Fwww.ubuntu-br.org%2F&twttr_widget=1&twttr_
      hask=0&twttr_li=0&twttr_pid= HTTP/1.1
Referer: http://platform.twitter.com/widgets/follow_button.1380141200.html
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR
Connection: Keep-Alive
Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5
Host: p.twitter.com

HTTP/1.1 200 OK
ETag: "377d257f2d2e294916143c069141c1c5:1328738114"
Last-Modified: Wed, 08 Feb 2012 21:55:14 GMT
Accept-Ranges: bytes
Content-Length: 43
Content-Type: image/gif
Cache-Control: no-cache
P3P: CP="CAO DSP LAW CURa ADMa DEVa TAIa PSAa PSDa IVAa IVDa OUR BUS IND UNI COM NAV INT"
Date: Sat, 28 Sep 2013 11:02:07 GMT
Connection: keep-alive
Set-Cookie: pid=v3:1380366127409323693130471; expires=Sun, 29-Mar-2015
      23:02:07 GMT; path=/; domain=.twitter.com

GIF89a...
```

http://www.ubuntu-br.org/
Set-Cookie
pid=v3:1380366127409323693130471
*.twitter.com até 29/03/2015

HTTP

```
GET /widgets/tweet_button.1380141200.html HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://blog.planalto.gov.br/queremos-tornar-o-governo-cada-vez-mais-
      digital-e-aberto-afirma-dilma-ao-lancar-o-novo-portal-brasil/
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/
Cookie: pid=v3:1380366127409323693130471
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR
Connection: Keep-Alive
Host: platform.twitter.com
```

http://blog.planalto.gov.br/
Cookie
pid=v3:1380366127409323693130471
platform.twitter.com

```
HTTP/1.1 200 OK
Content-Encoding: gzip
Cache-Control: public, max-age=315569260
Content-Type: text/html; charset=utf-8
Date: Sat, 28 Sep 2013 11:19:22 GMT
Etag: "87244c8ba90135256aba9064a79b2a9a+gzip"
Last-Modified: Wed, 25 Sep 2013 20:34:02 GMT
P3P: CP="CAO DSP LAW CURa ADMa DEVa TAIa PSAa PSDa IVAa IVDa OUR BUS IND UNI COM NAV INT"
Server: ECS (fll/0705)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 24992

<!DOCTYPE html>
```

HTTPS

- O protocolo HTTPS (HTTP+SSL) é muito seguro e não há nenhuma forma de obter os dados que trafegam através dele, por tratar-se de uma criptografia extremamente forte.
- Algumas empresas e alguns aplicativos o utilizam para garantir que possam espionar sem serem pegos.

HTTPS

MitmProxy

- É um sniffer para HTTPS;
- Funciona como um proxy Man-In-The-Middle;
- Gera os certificados para os sites em tempo real, com a configuração correta, os softwares não exibem erros de autenticidade.
- Ex: `# mitmproxy -w captura -T --host`

mitmproxy: a man-in-the-middle proxy

Intercept, modify, replay and save HTTP/S traffic

MITM – Android

```
2013-09-16 18:44:09 POST https://173.194.37.2/fdfe/bulkDetails
                        ← 200 application/x-gzip 106.25kB
Request                                                    Response
                                  25,shekel_test
X-DFE-Device-Id:                  3040fde9100a2a55
X-DFE-Client-Id:                  am-android-motorola
X-DFE-Logging-Id:                 -692e9a331d08d20
User-Agent:                       Android-Finsky/4.3.11 (api=3,versionCode=80230011,sdk=15,device=umts
                                  _spyder,hardware=mapphone_cdma,product=XT910_SEAOP)
X-DFE-SmallestScreenWidthDp:      360
X-DFE-Filter-Level:               3
Content-Length:                   2695
Host:                             android.clients.google.com
Connection:                       Keep-Alive
Protobuf
1: "at.tomtasche.reader"
1: "berserker.android.apps.sshdroidpro"
1: "br.com.banrisul.mbanking"
1: "br.com.gog.rastreadorencomendas"
1: "br.com.vivo"
1: "ch.serverbox.android.osciprime"
1: "com.adobe.flashplayer"
1: "com.almalence.hdr_plus"
1: "com.anddoes.fancywidgets"
[17/115]                                                   ?:help q:back [*:8080]
```

MITM – Teclado SWYPE / padrão da Motorola

```
2013-09-16 18:43:27 POST https://205.197.193.129/session/2/validate
                         ← 200 application/json 20B
Request                                                    Response
Content-Type:     text/json
Content-Length:   174
User-Agent:       Dalvik/1.6.0 (Linux; U; Android 4.0.4; XT910 Build/6.7.3-94_SPI-328)
Host:             api.swypeconnect.com
Connection:       Keep-Alive
Accept-Encoding:  gzip
Raw
{"sessionId":"7b7955f6-01ca-11e2-8d79-22000a6caf19","key":"R3JvbWl0LCB0aGF0J3MgaXRcISBDaGVlc2VcISBXZ
SdsbCBnbyBzb21ld2hlcmA","deviceId":"7ae9a548-32ca-19e2-8554-2227091c9e19"}

[2/115]                                                    ?:help q:back [*:8080]
```

DNS

1. Se o provedor sequestra, mude seu DNS, há uma lista de servidores com uma boa política de privacidade em http://www.opennicproject.org/
2. Use as possibilidades que o sistema lhe oferece:
   - Arquivo /etc/hosts
   - Cache de DNS, dnsmasq;
3. O dnsmasq permite wildcards, com a seguinte linha: `address=/dominio.alguma.coisa/0.0.0.1`
4. Em /etc/hosts, para bloquear uma máquina: `0.0.0.1 dominio.alguma.coisa`

HTTP/HTTPS – Extensões

Adblock Edge – Bloqueia propagandas e rastreadores, na configuração é possível baixar e definir o que deve ser bloqueado;

HTTPS Everywhere – Abre em HTTPS os sites que tem essa possibilidade;

Disconnect.me – Bloqueia sites que fazem rastreamento, atualmente suporta mais de 2000 serviços, tem aparência similar ao Ghostery;

Como se defender utilizando software livre na era da espionagem

Breno Neves

Dia da Liberdade de Software 2013

Setembro de 2013