



6ª SEMTEC

Semana de Tecnologia do
IFSP - *Campus Bragança Paulista*



INSTITUTO FEDERAL
SÃO PAULO

22 a 25 de outubro de 2013 - Instituto Federal de São Paulo - *Campus Bragança Paulista*

Contrainteligência | Segurança da informação | Forense Digital





Contraineligência | Segurança da informação | Forense Digital

ERASMO RIBEIRO GUIMARAES JUNIOR - ERGJ



Twitter: @erasmoguilmaras

Email: guimaraes.junior@menospapel.com.br

Facebook Perfil : ERASMOGUIMARAESJR

Facebook Pagina: Cyber Defesa (Educação, conscientização e prevenção cibernética)

Contraineligência, Segurança da Informação e Forense Digital

Erasmu Guimarães – Menos Papel & Cyberinvestigate – SP



Currículo: Pós Graduado em Direito Eletrônico pela Escola Paulista de Direito e Especialização Internacional em CyberSecurity and Law Program pela Caldwell Community College & Technical Institute (CCCTI-EUA), Extensão em Investigação e Fraude corporativa (Master Business Investigation and Fraud) pela Fundação Escola de Comércio Álvares Penteado (FECAP); Perito Forense Digital com larga experiência em Segurança de Informação, Tecnologia e Mitigação de riscos. Possui as principais certificações do mercado nacional e internacional como COBITc, ITILc, ACPFc (Axur security), CHFI - Computer Hacking Forensic Investigation pela EC-Council (EUA); Computer Forensic Investigations pelo SANS Institute (EUA).

Membro das entidades internacionais: HTCIA - High Technology Crime Investigation Association - Brasil, ACFE - Association Of Certified Fraud Examiners (EUA); ISSA - Information Systems Security Association - Capitulo Brasil; ISOC - Internet Society - Capítulos Brasil e Estados Unidos; Comissão de Direito Eletrônico e Crimes de Alta Tecnologia; Defesa e Cidadania da Ordem dos Advogados do Brasil - Seccção São Paulo;

Especializações: Gestor de Contraineligência e Segurança da informação da Menos Papel Serviços, Diretor de Tecnologia da ANARNET, Secretário Executivo da ONG - Instituto Coaliza, Secretário Adjunto da Comissão de Direito Eletrônico e Crimes de Alta Tecnologia da OAB/SP. Professor e palestrante para alunos de MBA, Pós Graduação e Graduação das Faculdade Alfa/FADISP; Mackenzie e UNIFEO, FMU, UNG, Subsecções da Ordem dos Advogados do Brasil.

Resumo do Palestra: Auditoria de TI, Gestão, Políticas e Regulamentos Interno de Segurança da Informação (PISI e RISI); Crimes cibernéticos, vazamento de dados; redes corporativas, hotéis; conexões remotas, sanitização de discos rígidos; e-mails anônimos; Scan, Scam, mitigação e de vulnerabilidades em redes corporativas; Contraineligência Corporativa; Forense & Anti-Forense Digital; Preservação de provas digitais, Cadeia de custodia; Aquisição/Duplicação de discos bit-a-bit (método Forense)método DOD 5220-22M.

HOJE – Realidade ou fantasia?



Qual pílula devo escolher hoje?

Vermelha = Conhecimento e sabedoria

Azul = Fantasia e a ficção

Missão – Trocar o Conhecimento (10%)

DAY OF REFLECTION

Número de malwares móveis e aplicativos de alto risco chega a 1 milhão

Dentre os aplicativos questionáveis encontrados, 75% executam rotinas maliciosas, enquanto que 25% realizam rotinas duvidosas - o que inclui adwares.



De acordo com um [relatório](#) de segurança da Trend Micro agora já existem 1 milhão de malwares para dispositivos móveis, como abusos de serviços Premium, e aplicativos de alto risco, que oferecem anúncios que levam a sites duvidosos de forma agressiva. Os dados analisados foram coletados pelo serviço de reputação de aplicativos para dispositivos móveis da empresa.

Principais Ameaças

Famílias de malware, tais como o FAKEINST (34%) e o OPFAKE (30%), são os principais códigos maliciosos usados em dispositivos móveis. Malwares FAKEINST normalmente aparecem disfarçados como aplicativos legítimos. Eles também são abusadores de serviços premium, que enviam mensagens de texto não autorizadas para determinados números e registram os usuários em serviços pagos.

Um incidente de grande repercussão envolvendo o FAKEINST são as falsas versões do Bad Piggies, encontradas logo após o lançamento do jogo.

O malware OPFAKE é semelhante ao FAKEINST, particularmente quanto à imitação de aplicativos legítimos. No entanto, uma variante - a ANDROIDOS_OPFAKE.CTD - mostrou um lado diferente do malware, criada para fazer com que usuários abrissem um arquivo HTML, onde são solicitados a baixar um arquivo possivelmente malicioso.

<http://goo.gl/dSybjB>

15 de outubro de 2013 - 08h00

INTRODUÇÃO GERAL

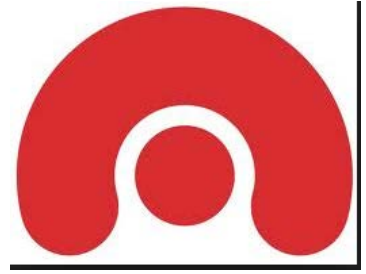
Menos  Papel



ArcSight 
An HP Company



Quem conhece?



Operation #AntiSec

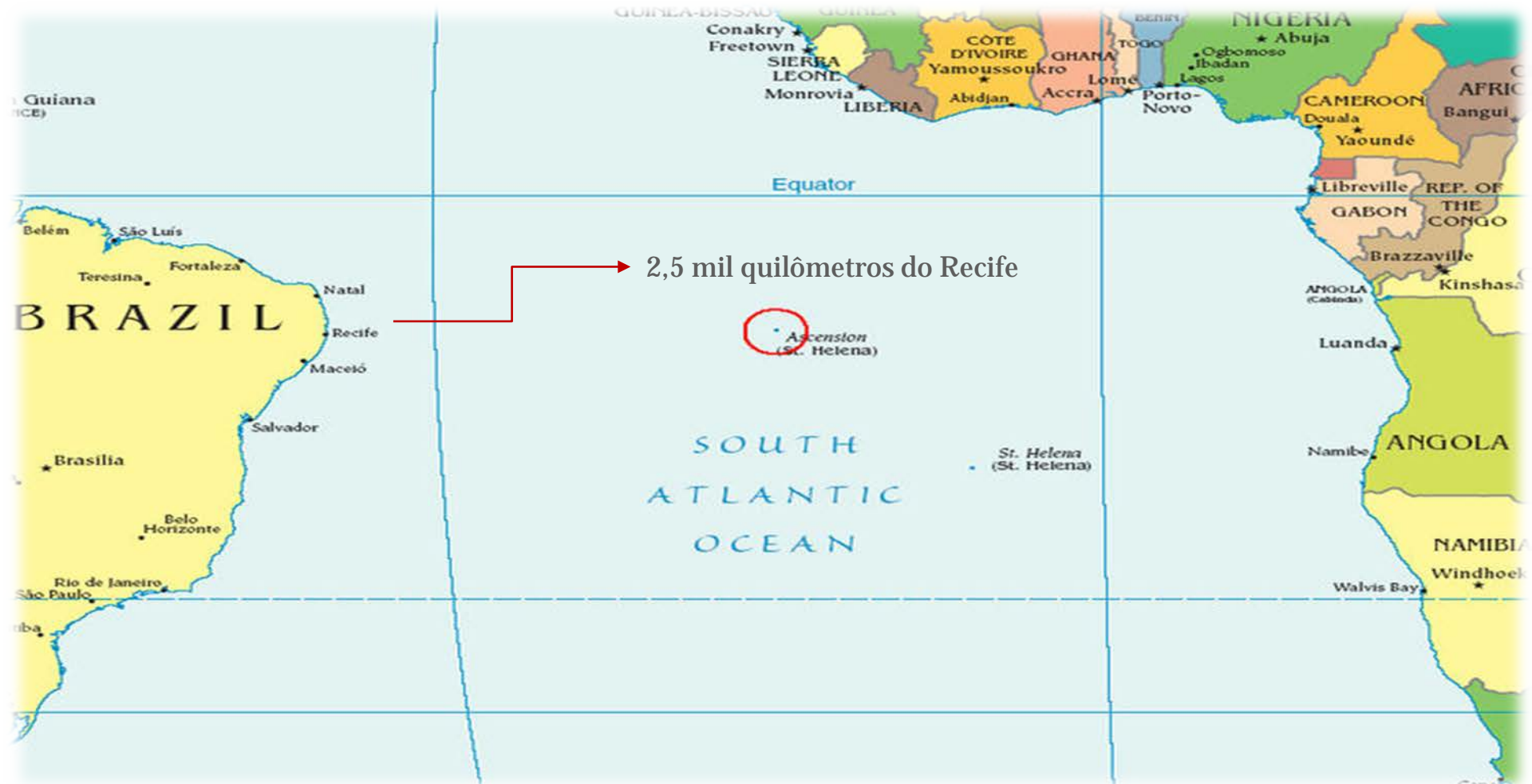






PRISM é um programa clandestino de vigilância eletrônica de massa *Data Mining Program* por ter sido operado pela Agência de Segurança Nacional dos Estados Unidos (NSA) desde 2007. [3] [4] [5] PRISM é um nome de código para o governo um esforço de coleta de dados conhecida oficialmente pelo **SIGAD US-984XN**

Ascension Island



Ilha de Ascensão, pequena ilha britânica no Oceano Atlântico Sul

Local estratégico utilizado para captar aproximadamente dois milhões de mensagens por hora, basicamente conversas telefônicas, troca de e-mails e posts em redes sociais. A ilha serviu á Inglaterra na Guerra das Malvinas.

#GCHQ

| Serviço de inteligência criptológica britânico

#ECHELON SYSTEM

Sistema existente desde 1946

Abastecido por 120 satélites para monitorar jefes de estado

“ E5 - Cynthia ”

The Counting Station - CIA

Base de comunicação com agentes secretos na América Sul e África

<http://goo.gl/qIDVgc>



(USA, GBR, AUS, CAN, NZL)

Estados Unidos, Reino Unido, Nova Zelândia, Austrália e Canadá

O PASSO A PASSO DA ESPIONAGEM



1

Na ilha de Ascensão, estrategicamente localizada no Atlântico Sul, superantenas captam dois milhões de mensagens por hora. São bilhões de sinais de comunicações de celulares, provedores e comunicações via satélite, os "megadados"

2

Os dados captados sofrem uma primeira análise na ilha e depois são encaminhados para Maryland e lançados em um computador que roda o programa Prism, capaz de decodificar os megadados e selecionar comunicações específicas de acordo com o interesse estratégico da NSA





4

Os dados são remetidos ao presidente e aos seus auxiliares mais próximos. Caso seja necessário monitorar as atividades específicas de pessoas ou grupos, considerados "ameaças" aos interesses americanos, a NSA aciona agentes locais que operam encobertos em várias partes do mundo

3

A NSA aciona as empresas parceiras, de telefonia e internet, para acessar o conteúdo desses dados, sejam eles e-mails, comunicações de voz sobre IP, ligações celulares, etc.



NDA

HASH

ESTEGANOGRAFIA

Esteganografia (do grego "escrita escondida") é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra, uma forma de [segurança por obscurantismo](#). Em outras palavras, esteganografia é o ramo particular da [criptologia](#) que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido.

WIPE

#NSA

National Security Agency

NSA Regional Security Operations Centers **(RSOCs)**

Fort Meade Regional SIGINT Operations Center Fort Meade, MD



[Georgia Regional Security Operations Center](#) Fort Gordon, GA



[Medina Regional Security Operations Center](#) San Antonio, TX



[National Reconnaissance Office complex](#) Aurora, CO



[Hawaii Regional Security Operations Center, Kunia, HI](#)



#CTRC

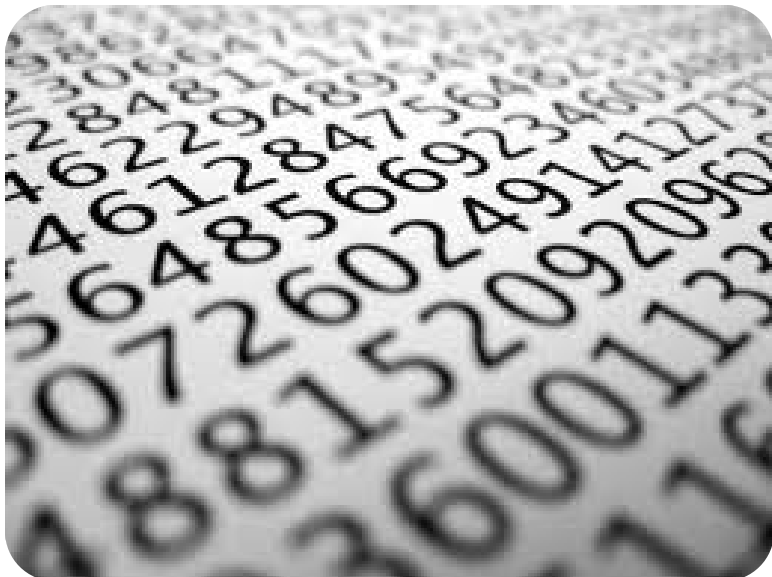
CyberTerrorism Response Center





#UVB-76

Uma radio que foi ativada desde o final de 1970. No inicio do anos 80 surgem os primeiros relatos da estação nesta frequência e a sua origem tem sido atribuída a [Rússia](#).



A radio fica online repetindo-se a um taxa de cerca de 25 tons por minuto, durante 24 horas por dia.

Hello kitty

X

Juan Carlos Ramírez Abadía



Mas quem é

Juan Carlos Ramírez Abadía?



Traficante colombiano

Quando foi preso em São Paulo, em agosto do ano passado, os delegados da Polícia Federal ficaram intrigados com a quantidade de imagens da gatinha japonesa que ele guardava nos computadores. Eram quase 200 imagens, quase todas enviadas por e-mail. A surpresa maior foi a descoberta de que a Hello Kitty não era só uma Hello Kitty. Havia mensagens de voz e de texto escondidas nas imagens. Algumas delas podem mudar o destino de Abadía no Brasil: **elas contêm ordens para movimentar cocaína entre países e para sumir com pessoas na Colômbia, segundo análise feita pelo DEA**, a agência antidrogas dos EUA. Para os americanos, Abadía continuou a comandar o tráfico na Colômbia mesmo após se mudar para o Brasil.





Depois de deixar o WikiLeaks, ele anunciou planos em janeiro de 2011 para abrir um novo site para anônimos vazamentos on-line chamado **OpenLeaks**



No Brasil, quase 70% não protege smartphone de maneira adequada, diz estudo

Informações são empresa de segurança McAfee, que também aponta que 81% dos entrevistados não adotam soluções de segurança abrangentes para seus tablete.



REFLEXÃO

Dados – Informação – Conhecimento – Sabedoria

Respostas mais utilizadas pelos gestores

1. Isto nunca acontecerá comigo, minhas informações estão seguras
2. Nunca fui atacado, não preciso de mais segurança
3. Já estou seguro com um Firewall
4. Não posso gastar com segurança agora, deixa assim mesmo
5. Ninguém vai descobrir essa “Falhinha” de segurança
6. Minha equipe já tem tudo sob controle
7. Aqui não possuo riscos com relação a fraude ou perda de receita
8. Utilizo os melhores (mais caros) sistemas de segurança, então eles devem ser seguros
9. Estes testes não são necessários para minha empresa

Nota: Os mitos citados são rapidamente derrubados e em geral são fundamentados por achometro



PAI HENRIQUE DO PC

TÉCNICO DE PCs, NOTEBOOKS e REDE

Consultas e trabalhos em geral
na Zona Sul de São Paulo

Trago o Windows de volta em 3 dias

EXORCISO PC FORMATADO POR SOBRINHO

Retiro vírus, malware e mau olhado
do seu computador ou Notebook

Recupero os mp3 e fotos
desinibidas escondidas

Fecho a sua rede contra olho
gordo e trago sinal wifi do além

**Mais de 6.000 Windows Ressuscitados!
Sofre com Lentidão e travamento?
Pare agora de sofrer!**

Pagamento somente após resultado

- Técnicos de Confiança?
- Assinou o NDA?
- Existe garantias da confidencialidade das suas informações?

Lembre-se:

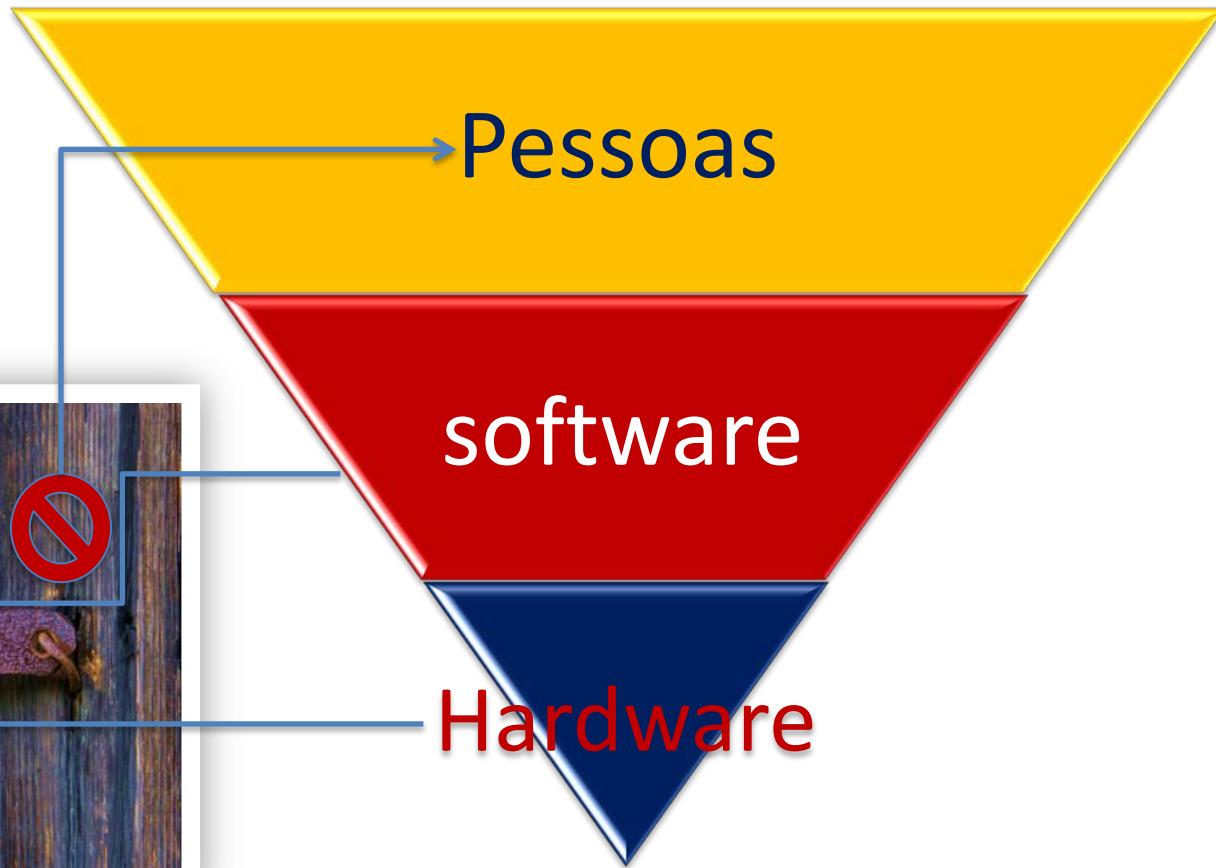
Projetos e atividades críticas devem ser realizadas por especialista.

É Recomendo muita atenção e cuidado com os profissionais genéricos.



Mundo Atual

1ª VISÃO HOLÍSTICA



Onde esta a Vulnerabilidade?



- ✓ Falsa sensação de segurança
- ✓ Relação de Confiança (Achômetro)
- ✓ Crença infundada - Sofismo
- ✓ Acreditar que nunca vai acontecer
- ✓ Crer que só acontece com os outros
- ✓ Gestão baseada na reação
- ✓ Excesso de Confiança
- ✓ Negligência, imperícia e imprudência... (Culpa)



Agrega valor na mitigação de riscos e boas praticas



ITIL
COBIT

PCI-DSS - Payment Card Industry Data Security Standard (Visa, MasterCard , JBC, Discover, American Express) - é composta de 12 requisitos destinados a proteger os sistemas de negócios que armazenam, processam ou transmitem dados do titular do cartão e destina-se a proteger os consumidores e comerciantes contra violações de segurança.

CVM - Comissão de Valores Mobiliários

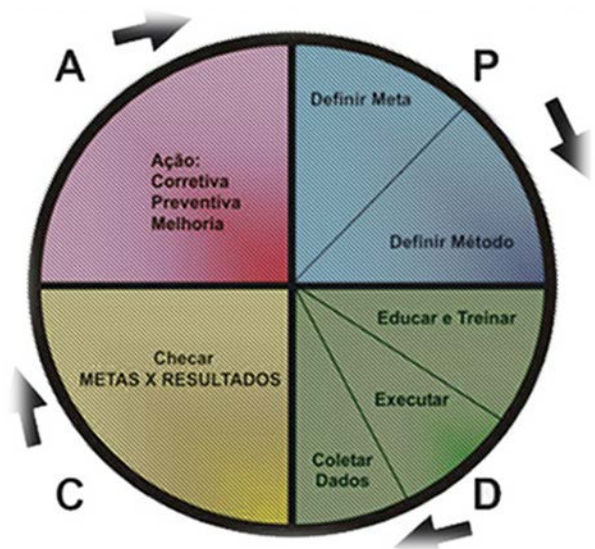
SEC - Securities and Exchange Commission (**Comissão de Valores Mobiliários**)

SOX – **Sarbanes - Oxley** - garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas

BASILEIA II - Objetivo de buscar uma medida mais precisa dos riscos incorridos pelos bancos internacionalmente ativos.

COSO - Committee of Sponsoring Organizations – Gestão de Risco Corporativo

Agrega valor na mitigação de riscos e boas praticas



ISO 27001

Esta é a especificação para um sistema de gestão de segurança da informação (ISMS um), que substituiu a antiga norma BS7799-2

ISO 27003

Este será o número oficial de um novo padrão pretende oferecer orientação para a implementação de um SGSI (IS Management System).

ISO 27005

Este é o padrão ISO independente metodologia de gestão de riscos de segurança da informação. .

ISO 27002

Este é o número padrão 27000 série do que era originalmente a norma ISO 17799 (que por si só era anteriormente conhecida como BS7799-1). .

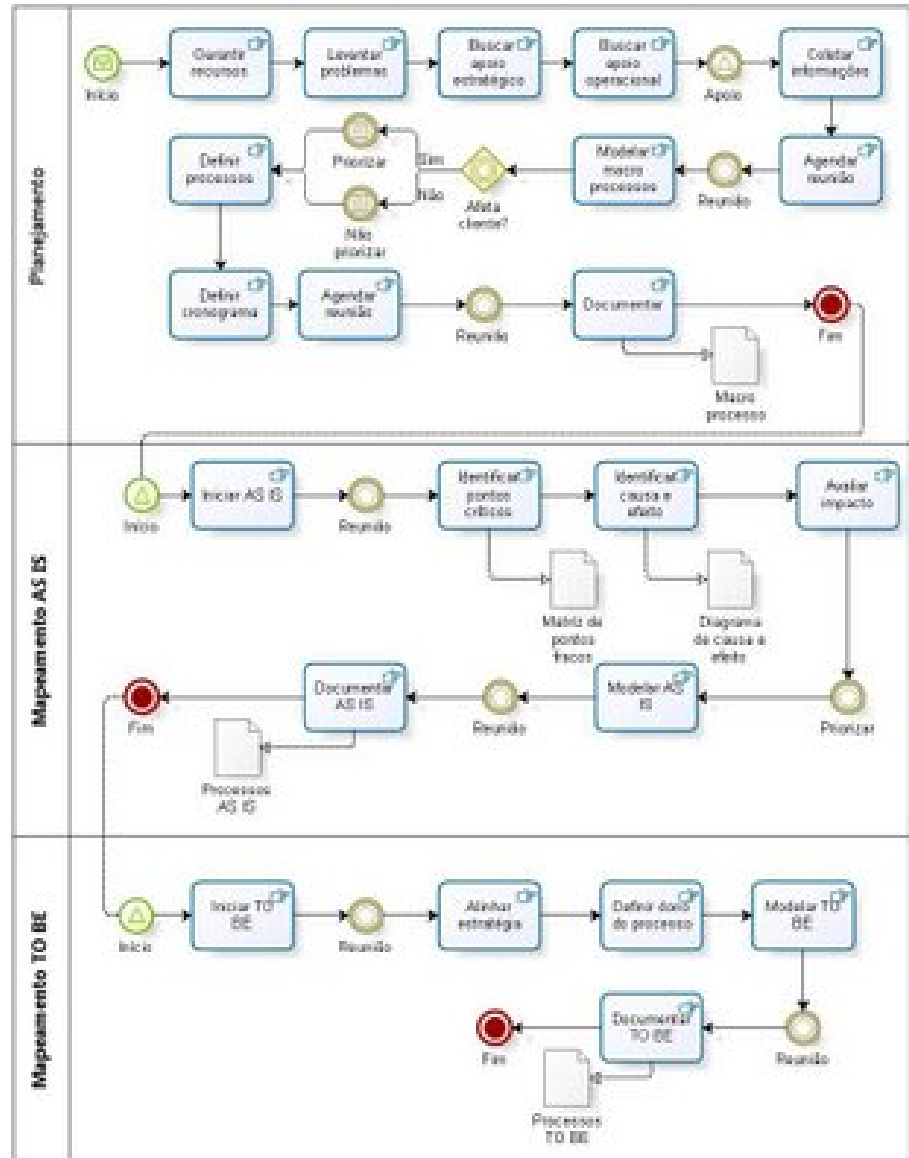
ISO 27004

Esta norma abrange informações de segurança de medição do sistema de gestão e métricas, incluindo ISO27002 controles alinhados sugeridas..

ISO 27006

Esta norma fornece diretrizes para o credenciamento de organizações que oferecem certificação do SGSI.

Entrevistas
Desenhos
Modelagem
=
Processo



O que vai parar no Lixo?



Qual o valor do seu Lixo?
Quanto o seu concorrente pagaria pelo seu Pseudo-lixo?



DESCARTE DE LIXO E MÍDIAS

Dados – Informação – Conhecimento – Sabedoria

Prestadores de Serviços

(Vazamento de dados sensíveis)



- **Dados sensíveis?**
- **Sanitização?**
- **Leilão do legado?**



Assumir o Risco?
Transferir o risco?
Mitigar o Risco?



HOME OFFICE E SEUS RISCOS

Mundo Corporativo & Vida Cotidiana – Riscos e Oportunidades

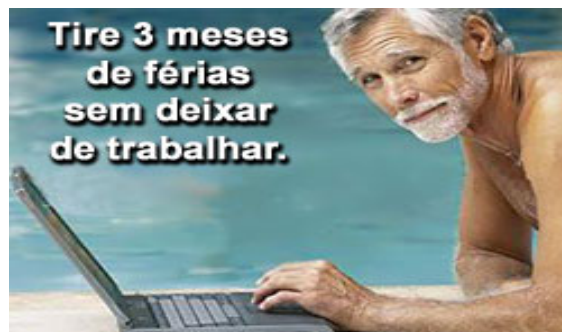


ASSINOU O NDA
Non-disclosure agreement

Solução de Teletrabalho



Os colaboradores da sua empresa conseguem trabalhar a partir de casa se for necessário?





BYOD - CONSUMERIZAÇÃO

Dados – Informação – Conhecimento – Sabedoria

Vazamento de informações sensíveis

1MB >> 3TB
HOJE



Pendrives e cartões SD são responsáveis por 30% das infecções em PCs

Ataques por meio desses dispositivos podem servir para espalhar vírus e para roubar informações diretamente das máquinas



CYBER CRIMES

Dados – Informação – Conhecimento – Sabedoria

Um estudo realizado em 24 países pela divisão Norton da Symantec revelou que o custo total do cibercrime no mundo é de aproximadamente **US\$ 388 bilhões por ano**. Esse valor inclui **US\$ 114 bilhões em roubos** diretos e resposta a ataques e outros **US\$ 274 bilhões** referentes ao tempo perdido pelas vítimas desse tipo de crime.

O estudo **Norton Cybercrime Report 2011** entrevistou mais de **19 mil pessoas**. A estimativa é de que, no Brasil, o custo do cibercrime foi de **US\$ 15 bilhões em roubos** diretos e **US\$ 48 bilhões** em tempo de resposta aos ataques. Nos Estados Unidos, esses custos foram de **US\$ 32 bilhões diretos e US\$ 108 bilhões em respostas**

Em todo o mundo, **589 milhões** de pessoas foram afetadas, **431 milhões** apenas nos últimos 12 meses. São **1 milhão** de pessoas por dia vítimas de cibercrime.

Segundo estimativas, o tráfico internacional de drogas movimentada aproximadamente **US\$ 411 bilhões** em todo o mundo. O relatório da Norton diz que o cibercrime já superou o total de vendas de maconha e cocaína no mercado negro.

Criminal infiltration of financial institutions

BARRERA BARRERA & GUERRERO CASTILLO Organizations

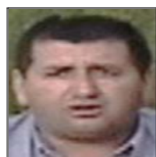
March 2010

U. S. Department of the Treasury
Office of Foreign Assets Control

Foreign Narcotics Kingpin
Designation Act ("Kingpin Act")

Red text indicates
previously-identified
Kingpin Act designees

Colombia's Most Wanted Drug Traffickers List



Daniel BARRERA BARRERA
(a.k.a. "El Loco Barrera")
DOB 06 Nov 1968
Alt. DOB 15 Sep 1967
CC 18221599 (Colombia)



Pedro Oliveira GUERRERO CASTILLO
(a.k.a. "Cuchillo")
DOB 28 Feb 1970
POB San Martin, Meta, Colombia
CC 17355451 (Colombia)

Drug Trafficking Partners with the FARC



FUERZAS ARMADAS REVOLUCIONARIAS DE COLOMBIA (a.k.a. FARC)

Assets in Narcotics Trafficking Activities

President
CARI LLANCA S.A.
Costa Rica



Partner, Manager
CARI LLANCA COLOMBIA Y CIA.
Colombia

Treasurer

Partner, Deputy Manager



EJERCITO REVOLUCIONARIO POPULAR ANTI TERRORISTA DE COLOMBIA (a.k.a. ERPAC)

Leader

Area of Influence



Illegal armed group operating in Eastern Colombia; categorized by Colombian authorities as a **BACRIM** - "Banda Criminal".
EFFPAC has influence in the Colombian Departments of Meta, Guaviare, Vichada, and Guainia (Outlined in black). The last two border Venezuela.



Arrested by Colombian Authorities in 2009 on Drug Trafficking and/or Money Laundering Charges and Remain in Custody

BARRERA BARRERA's Key Criminal Collaborators

 Danilo BUSTOS SUAREZ DOB 11 Sep 1963 CC 79203879 (Colombia)	 Armando GUTIERREZ GARAVITO DOB 02 Dec 1959 POB Acadia, Meta, Colombia CC 17410782 (Colombia) N.I. E. X-1552120-B (Spain)	 Wilmer OSPINA MUIRI LLO DOB 26 May 1970 CC 17344677 (Colombia)	 Tullio Adan ARIOSTI ZABALA GIRALDO DOB 06 Mar 1966 Alt. DOB 03 Jun 1966 CC 78395721 (Colombia)
---	--	--	---

BARRERA BARRERA's Key Money Launderers

 Jaime JEREZ GALEANO DOB 08 Apr 1969 POB Bogota, Colombia CC 79484852 (Colombia)	 Oscar Alberto JEREZ PIEDRA DOB 07 Aug 1968 POB Bogota, Colombia CC 79133740 (Colombia)	 Oscar Richard MARTINEZ ARAANGO DOB 31 Jul 1972 CC 79634329 (Colombia)
--	---	---

BARRERA BARRERA's Key Front Persons

 Jesus Antonio SERNAL LONDONO DOB 10 Apr 1943 POB La Ceja, Antioquia, Colombia CC 2911166 (Colombia)	 Hernan Darío ARAANGO MADROÑAL GAL DOB 20 Mar 1952 POB Yarumal, Antioquia, Colombia CC 19186993 (Colombia)	 Jose Lenin AGUILAR DUARTE CC 79265614 (Colombia) Res. 117000439417 (Costa Rica)	 Meías SALAMANCA BUITRAGO DOB 05 Jun 1951 Alt. DOB 01 May 1951 CC 19133648 (Colombia)	 Jesus Antonio LONDONO ZAPATA DOB 24 Aug 1954 CC 6633775 (Colombia) Ex-Elected Representative to the Meta Department Assembly
--	--	---	---	---

GUERRERO CASTILLO's Key Front Persons

 Oscar de Jesus LOPEZ CADAVID DOB 21 Jun 1956 CC 10956431 (Colombia) Ex-Governor of Guaviare Department (In Colombian custody)	 Nelio de Jesus ECHEBERRY CADAVID DOB 28 Nov 1944 CC 10956431 (Colombia) Ex-Governor of Guaviare Department
--	---

Key Companies Related to BARRERA BARRERA*

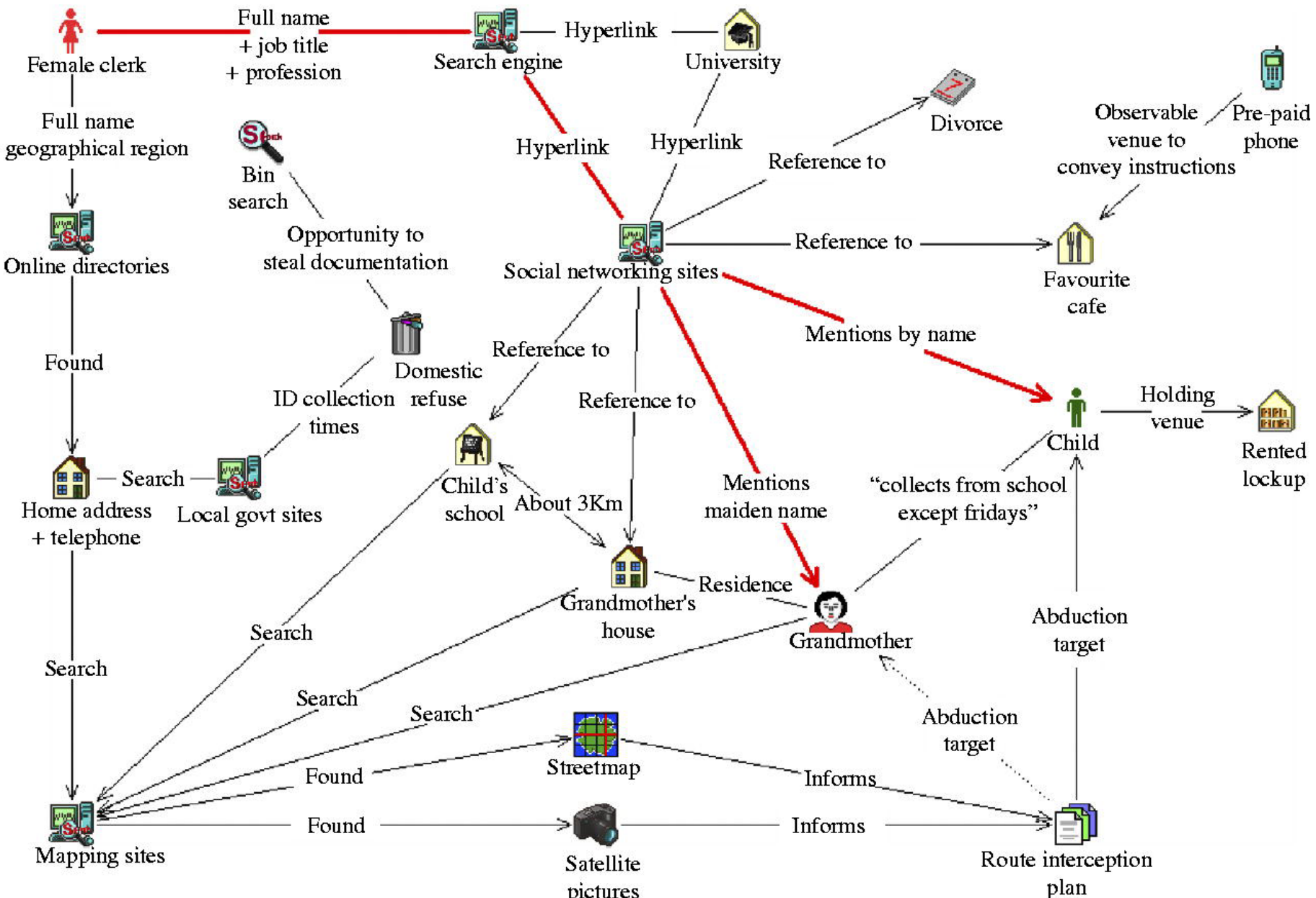
 HEPHEZ LTDA. (a.k.a. CARNES GUERNAVACA) Bogota, Colombia NIT # 900083653-1 (Colombia)	 MATAMBRE DE LO MEJOR Bogota, Colombia Matricula Mercantil No 1664511 (Colombia)	 INVERSI ONES TALADRO LTDA. (a.k.a. KUARZO DI SCOTEGA) Villavicencio, Colombia NIT # 900063810-0 (Colombia)	 COLPRETINAS LTDA. (a.k.a. CP TEXTILES) Bogota, Colombia NIT # 830034149-6 (Colombia)
 BINGO INTERNACIONAL EU. Bogota, Colombia NIT # 900103490-3 (Colombia)	 BLUE STAR SEGON HOSTELERI S.L. Paris, Madrid 28981, Spain C.I.F. B84214477 (Spain)	 C.A. COMERCIALIZADORA DE MOTOCICLETAS Y REPUESTOS S.A. (a.k.a. WISMOTOS S.A.) Villavicencio, Colombia NIT # 900069501-0 (Colombia)	 COMERCIALIZADORA DE CARNES MGG LTDA. (a.k.a. CARNES EL PROVEEDOR C.F.P.; CARNES LA MONDIAL M.A.) Villavicencio, Colombia NIT # 830108927-9 (Colombia)
 CRIADERO EL TAMBO LTDA. Bogota, Colombia NIT # 900016185-9 (Colombia)	 CULTIVARI S.A. Fuente de Oro, Meta, Colombia NIT # 822007334-9 (Colombia)	 DEWELLE CENTRO DE ESTETICA Y BELLEZA LTDA. Bogota, Colombia NIT # 900049690-9 (Colombia)	 COMERCIALIZADORA EI NVERSI ONES BUSTOS ARI ZA Y CIA S.C.S. (a.k.a. TRANSGEBA) Bogota, Colombia NIT # 830084978-9 (Colombia)
 JAI ME JEREZ Y CIA S.C.S. JERGAL S.C.S. Bogota, Colombia NIT # 860525034-4 (Colombia)	 JESBEL Y CIA S. ENC. Cota, Cundinamarca, Colombia NIT # 860525699-0 (Colombia)	 LOGISTICA Y TRANSPORTE NORVAL LTDA. Bogota, Colombia NIT # 900224846-0 (Colombia)	 GESTION ALFA LTDA. Bogota, Colombia NIT # 830095836-9 (Colombia)
 LOGISTICA Y TRANSPORTE NORVAL LTDA. Bogota, Colombia NIT # 900224846-0 (Colombia)	 MODERNA EXPRESS TRANSPORTE DE CARGA LTDA. Bogota, Colombia NIT # 830039006-4 (Colombia)	 INVERSI ONES GANADERAS Y PALMERAS S.A. (a.k.a. GANAPALMAS S.A.) Bogota, Colombia NIT # 900016274-6 (Colombia)	 PANCO Y SEDAS LTDA. (a.k.a. TELARAMA A Y S) Bogota, Colombia NIT # 830070893-0 (Colombia)

Companies Related to GUERRERO CASTILLO

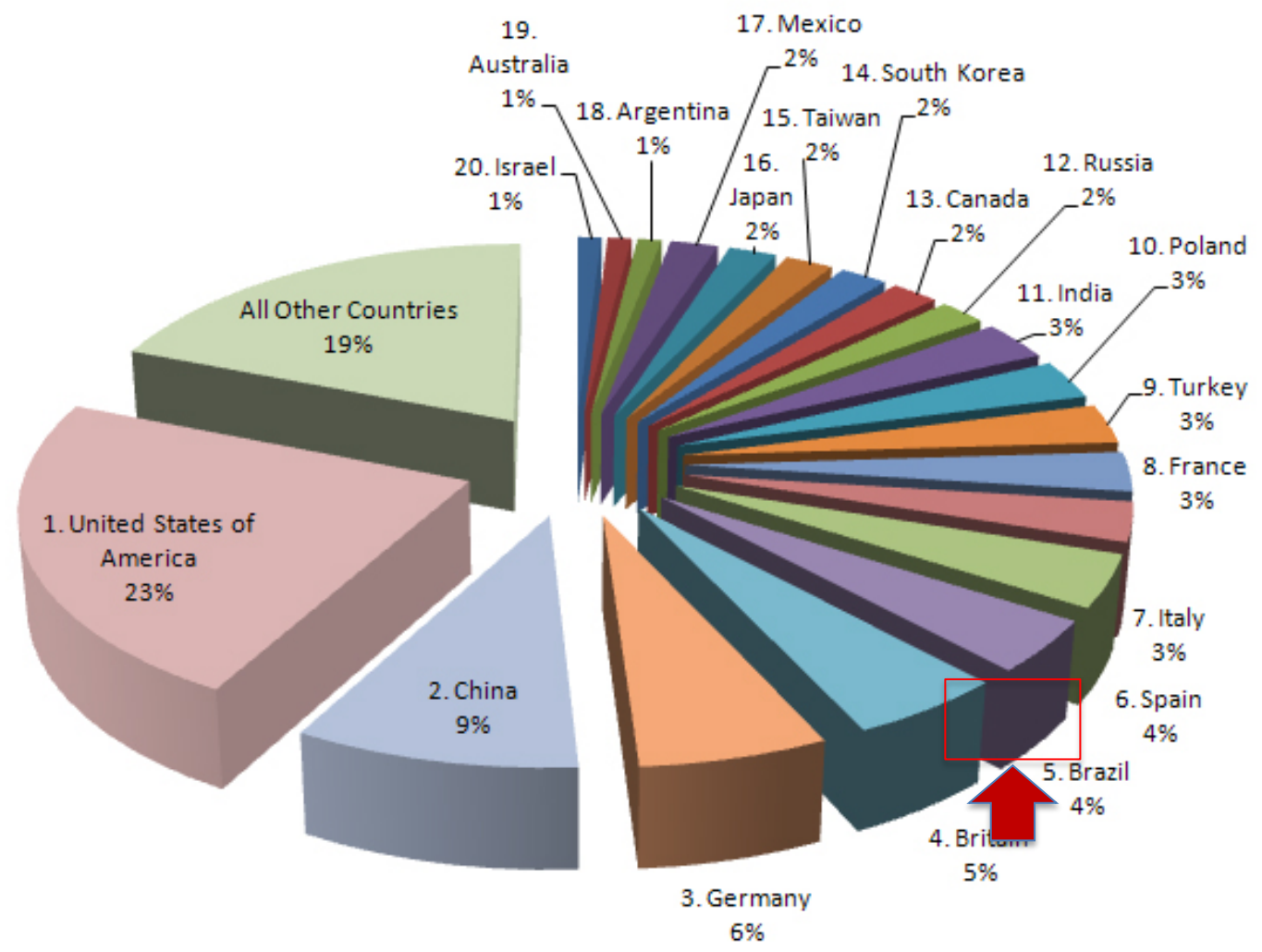
 EL PROVEEDOR SUPERMERCADOS EL PROVEEDOR
 PROVEEDORES Y DISTRIBUIDORES NACIONALES S.A. (a.k.a. NACIONAL DISTRIBUCIONES; PRODSINAL S.A.; PROVEEDOR HOGAR) Yopal, Casanare, Colombia Puerto Iguiria, Guainia, Colombia Granada, Meta, Colombia San Jose del Guaviare, Guaviare, Colombia Villavicencio, Colombia Bogota, Colombia NIT # 830511666-9 (Colombia)
 HACIENDA VENDOVAL Verda Patona Km. 2 Paratebueno, Cundinamarca, Colombia Matricula Mercantil No 1473503 (Colombia)

* (25 other entities related to BARRERA BARRERA were also designated)

Criminal infiltration of financial institutions



PRIVACIDADE + EXPOSIÇÃO + OPORTUNIDADES = CYBERCRIME



Cybercrime: Top 20 Countries



PASTEBIN

[CREATE NEW PASTE](#) [TRENDING PASTES](#)**A13xGO - COMEDIAAAAAA**

BY: A GUEST | MAR 21ST, 2010 | SYNTAX: MIRC | SIZE: 7.60 KB | VIEWS: 183 | EXPIRES: NEVER

[COPY TO CLIPBOARD](#) | [DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#)

EM TODO COMPRADOR TEM UM VENDEDOR
SAIBA QUEM VOCÊ É NA WWW.OLX.COM.BR



```
1. [18:12:46] 1<12@A13xGO1> ircbr.org
2. [18:12:46] 1<2ForaDaLeil> é voc
3. [18:12:47] 12<02naressii12>1 kkkk
4. [18:12:48] 1<2ForaDaLeil> que ofaa gige
5. [18:12:48] 12<02naressii12>1 coitado
6. [18:12:49] 12<02naressii12>1 coitaaaaaaado
7. [18:12:50] 1<2ForaDaLeil> auhehuaheuaheuaheuaheuaheuaheuaheua
8. [18:12:51] 12<02naressii12>1 AOEHAOEIHEAOIHEAIOHEAIOh
9. [18:12:55] 12<02naressii12>1 tenho dó e você A13xGO
10. [18:12:56] 1<12@A13xGO1> cala a boca
11. [18:12:57] 12<02naressii12>1 acha que sou noob
12. [18:12:58] 1<12@A13xGO1> mafiath.com
13. [18:12:59] 1<12@A13xGO1> ircbr.org
14. [18:13:00] 12<02naressii12>1 que nem o foradalei
15. [18:13:02] 12<02naressii12>1 AEHAEUIAEHIUEAHAUEIHEAUIHEAUIEHAUEAH
16. [18:13:04] 12<02naressii12>1 kkkkkkkkkkk
17. [18:13:05] 12<02naressii12>1 procura
18. [18:13:06] 1<12@A13xGO1> athbrazil.com
19. [18:13:10] 1<12@A13xGO1> fullnetwork.org
20. [18:13:14] 12<02naressii12>1 procura minhas botnet ae
21. [18:13:16] 12<02naressii12>1 vai la
22. [18:13:19] 12<02naressii12>1 pacota tudo essas
```

VIDEO HACKER DE SMTP FAZENDO VITIMAS NA INTERNET

<http://www.sonovela.net/video/1yU0iKEj5p4/Servidor-smtp-By-Al3xG0.html>

LINKS CRIMINAIS AL3XG0

MERCADORIAS ROUBADAS NA INTERNET E PEOFILIA

SITE AL3XG0 COM BANDEIRA MASTERCARD

VIDEO ENSINANDO A FAZER VITIMAS NA INTERNET DIRETAMENTE DA REDE DE BATEPAPO SECRETA IRC.SILVERLORDS.ORG

PUBLICAÇÕES

AL3XG0
 Feb 01, 2011
 ALEXANDRE BRASIL DE ABREU & CONHECIDO POPULARMENTE NO MUNDO DO CRIME COMO AL3XG0 PORTADOR DO RG: 62.3434.1963 & CPF: 096.023.577-97 RESIDENTE NO RESIDENCIAL ELDORADO - GOIANIA - ...
[Continue >>](#)

terça-feira, 1 de fevereiro de 2011

AL3XG0



ALEXANDRE BRASIL DE ABREU

CONHECIDO POPULARMENTE NO MUNDO DO CRIME COMO AL3XG0

PORTADOR DO RG: 62.3434.1963 E CPF: 096.023.577-97

RESIDENTE NO RESIDENCIAL ELDORADO - GOIANIA - GO

PRATICANTE DE UM RITUAL CRIMINOSO, QUÊ É DE FAZER VITIMAS NA INTERNET, SEJA DIRETA OU

ESTATISTICAS

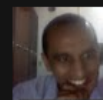
Hoje 147

Total 1273

Online 12

 12 Brazil

POSTAGENS



AL3XG0
 ALEXANDRE BRASIL DE ABREU
 CONHECIDO

POPULARMENTE NO MUNDO DO CRIME COMO AL3XG0 PORTADOR DO RG: 62.3434.1963 E CPF: 096.023.577-97

sexta-feira, 24 de junho de 2011

junho de 2011

D	S	T	Q	Q	S	S
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

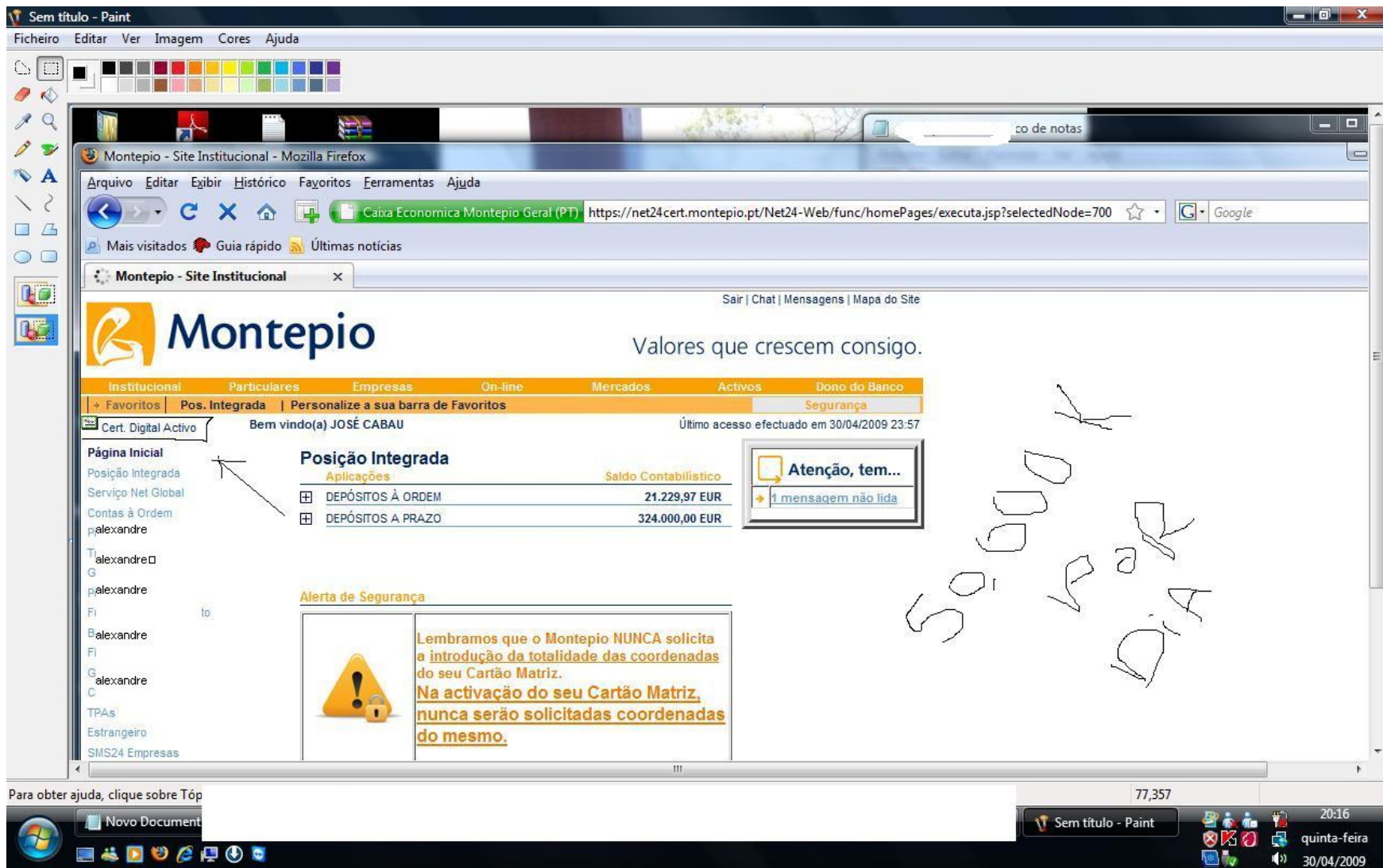


04:50:57

[Alterar configurações de data e hora...](#)

```
[01:10:42] * Mussego esta away, Tulliii ver a mãe depois eu voltooooooooooooo ,p
desde[23:00:02] site[n/a] email[none@none] uin[none] log[on] pager[off] --[Cyber]==
[01:10:55] x7x hxr se foi: [Quit:]
[01:11:23] <&CHOBAN> * Numero: 9993 marciomarkman@hotmail.com OK
[01:11:23] <&CHOBAN> * Numero: 9994 marco.maciuel@senado.gov.br OK
[01:11:23] <&CHOBAN> * Numero: 9995 marco.mazzoni@sefaz.pe.gov.br OK
[01:11:23] <&CHOBAN> * Numero: 9996 marco-forkin@casamilitar.rs.gov.br OK
[01:11:23] <&CHOBAN> * Numero: 9997 marco-forlin@casamilitar.rs.gov.br OK
[01:11:23] <&CHOBAN> * Numero: 9998 marcomedeiros@codeba.com.br OK
[01:11:23] <&CHOBAN> * Numero: 9999 marcos.moreira@integracao.gov.br OK
[01:11:29] <&CHOBAN> cannabis
[01:11:31] <&CHOBAN> fila
[01:11:32] <&CHOBAN> da puta
[01:11:36] <&CHOBAN> vai mi desenrola
[01:11:37] <&CHOBAN> um cc
[01:11:38] <&CHOBAN> ?
[01:11:40] <&CHOBAN> cannabis
[01:11:41] <&CHOBAN> cannabis
[01:11:41] <&CHOBAN> cannabis
[01:11:42] <&CHOBAN> cannabis
[01:11:42] <&CHOBAN> cannabis
[01:11:43] <&CHOBAN> cannabis
[01:12:31] <build> Preciso de SOURCE de AUTO ENVIO em DELPHI, utilizando SMTP (Uol,
Terra).. funcionando com logins de senhas diferentes.. enviando bonitinho.. pode
estar com av pegando.. nao tem problema.. troco por source de WORMWAB filezinho sem
av pegando enviando por FTP ou LOADER PRIV8 puxando 2links 17kb nao comprimido.
[01:13:17] * Entrou: IRCDIG [IRCDIG@344AA2E1.C1628FF0.81199C9F.IP]
[01:15:01] <&CHOBAN> * Numero: 5708 eveliseribas@ig.com.br OK
[01:15:02] <&CHOBAN> * Numero: 5709 fabianomache@terra.com.br OK
[01:15:02] <&CHOBAN> * Numero: 5710 fabianomcb@uol.com.br OK
[01:15:02] <&CHOBAN> * Numero: 5711 fabioaugusto.borba@bol.com.br OK
[01:15:11] <%Total190> Cabe de começar.
[01:15:11] <&CHOBAN> Quero cc br
[01:15:12] <&CHOBAN> Quero cc br
[01:15:12] <&CHOBAN> Quero cc br
[01:15:12] <%Total190> Caixa de entrada (3)
[01:15:12] <%Total190> Com estrela
[01:15:12] <&CHOBAN> Quero cc br
[01:15:12] <&CHOBAN> Quero cc br
[01:15:15] <%Total190> ^^
```

```
~netinho
&CHOBAN
&IRCBR
&J4AICA
@BOLADAO
@delet
@Echo-OFF
@Juliana
@JuniorSantos
@mendes_rs
%bnk
%Total190
+Governador
[SoLiTaRi0]
aguniado
Artu-Dormiu
azambzumbz
bnd
build
COKE
corvo
CyberScript32_
ilsnss
IOnkaster
IRCDIG
Koal4
Mal
MaldadeBr_OFF
Mussego
natan
Neu_rox
newbao
nina
Panicow
psy
RafaelziN
Rodrigo
Seven
simao
cinetra
```

Sem título - Paint

Ficheiro Editar Ver Imagem Cores Ajuda

Montepio - Site Institucional - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

Caixa Económica Montepio Geral (PT) <https://net24.cert.montepio.pt/Net24-Web/func/homePages/executa.jsp?selectedNode=700> Google

Mais visitados Guia rápido Últimas notícias

Montepio - Site Institucional

Sair | Chat | Mensagens | Mapa do Site

Montepio

Valores que crescem consigo.

Institucional Particulares Empresas On-line Mercados Activos Dono do Banco

Favoritos Pos. Integrada Personalize a sua barra de Favoritos Segurança

Cert. Digital Activo Bem vindo(a) JOSÉ CABAU Último acesso efectuado em 30/04/2009 23:57

Página Inicial

Posição Integrada

Serviço Net Global

Contas à Ordem

palexandre

Talexandre

Galexandre

palexandre

Falexandre

Falexandre

Galexandre

Calexandre

TPAs

Estrangeiro


SMS24 Empresas

Posição Integrada

Aplicações	Saldo Contabilístico
DEPÓSITOS À ORDEM	21.229,97 EUR
DEPÓSITOS A PRAZO	324.000,00 EUR

Atenção, tem...
1 mensagem não lida

Alerta de Segurança

 Lembramos que o Montepio **NUNCA** solicita a introdução da totalidade das coordenadas do seu Cartão Matriz. **Na activação do seu Cartão Matriz, nunca serão solicitadas coordenadas do mesmo.**

SÓ PARA DIÁ

Para obter ajuda, clique sobre Tóp

Novo Document

77,357

Sem título - Paint

20:16

quinta-feira

30/04/2009



TOR – NAVEGAÇÃO ANONIMA

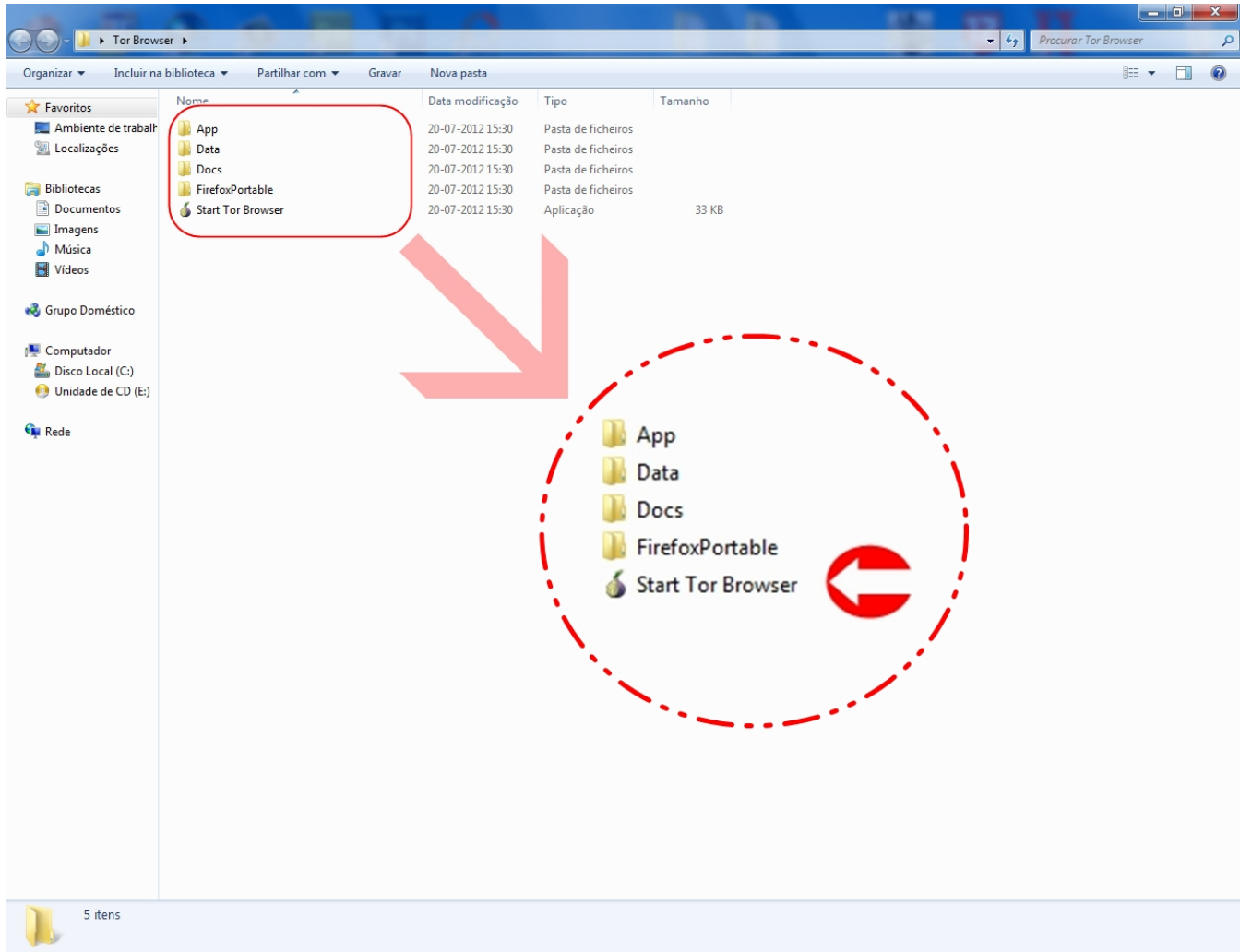
Dados – Informação – Conhecimento – Sabedoria

QUEM UTILIZA ESTA FERRAMENTA?



POR QUE?

TOR

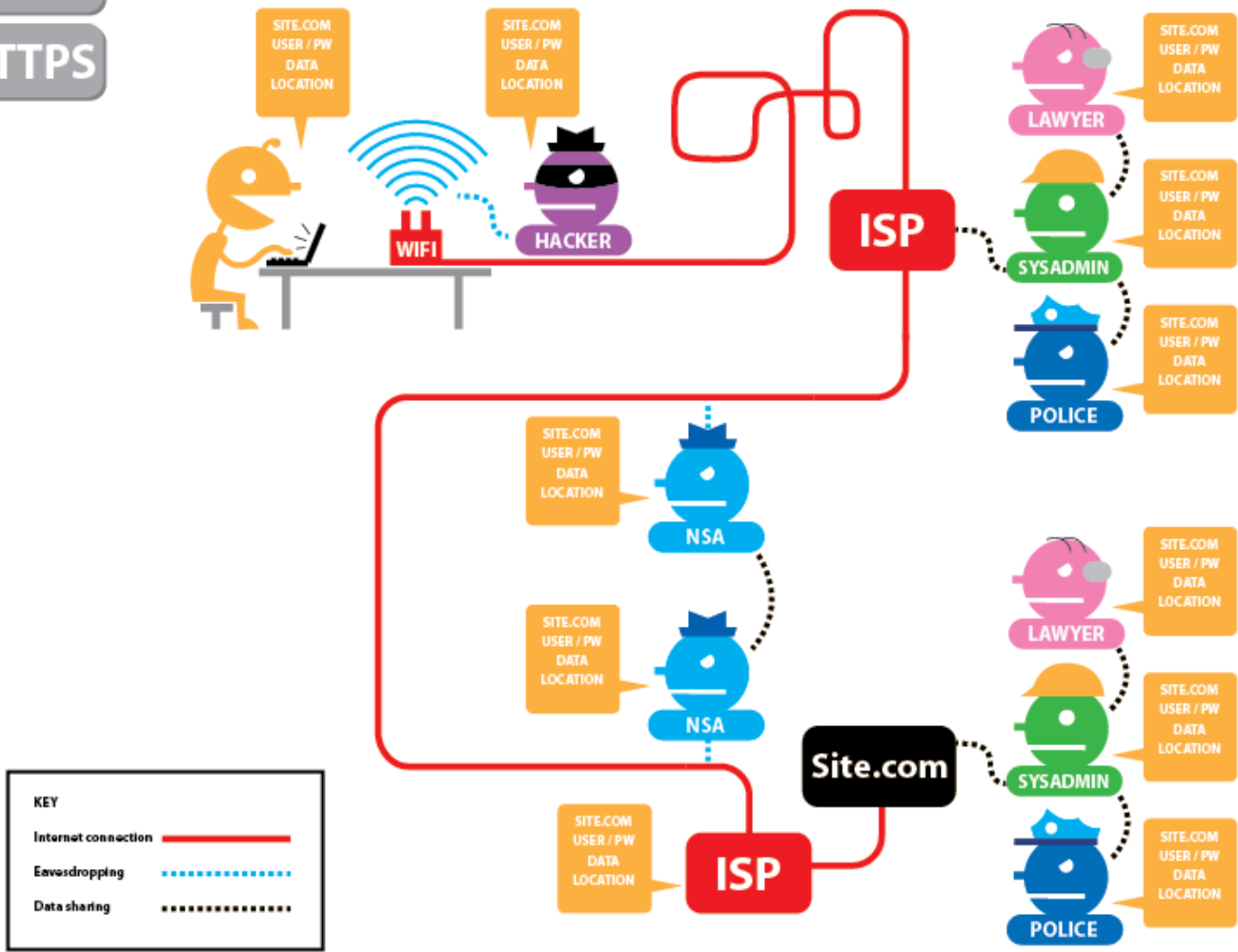


TOR



NAVEGAÇÃO EM SITES SEM HTTPS

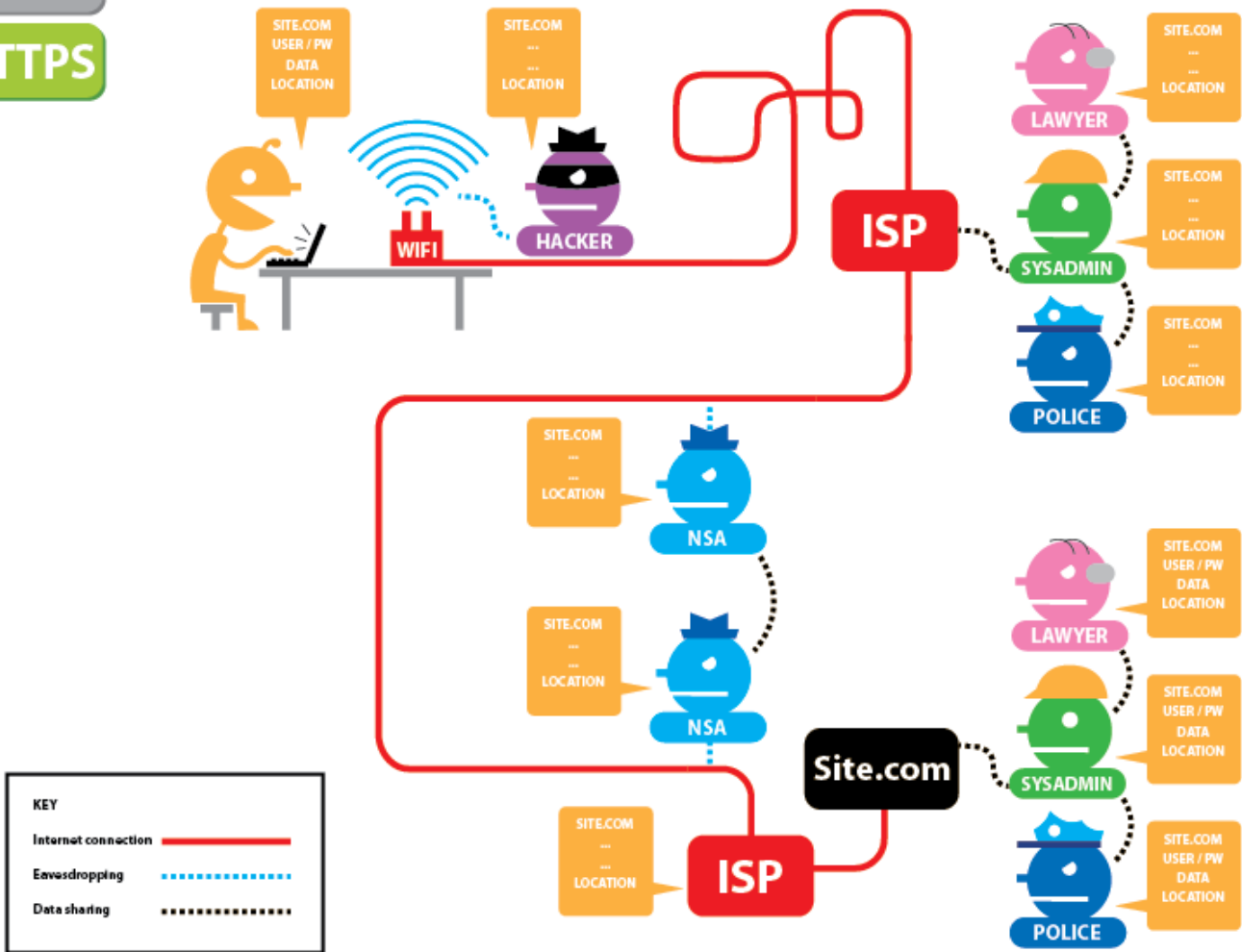
Tor
HTTPS



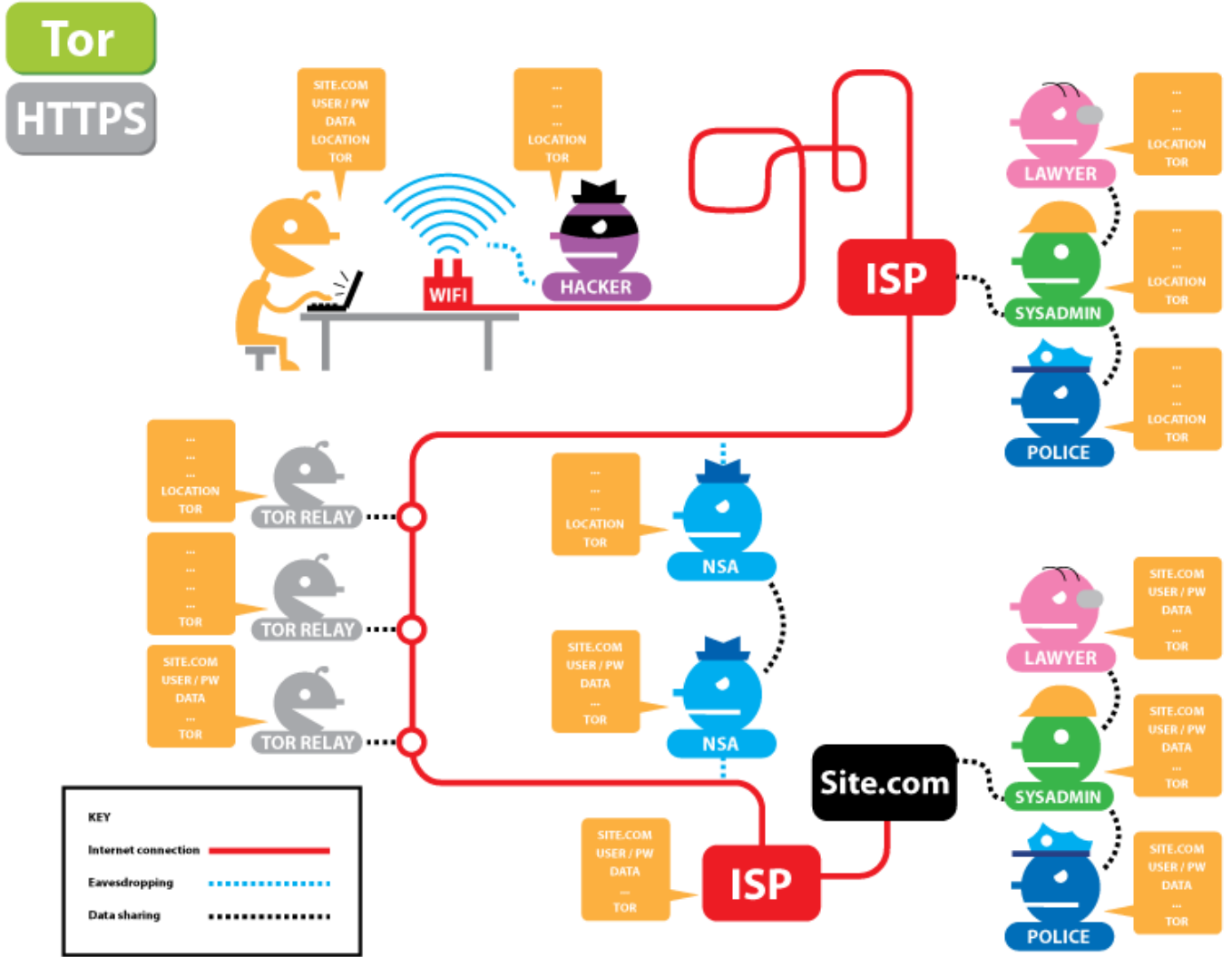
<https://www.eff.org/pages/tor-and-https>

TOR NAVEGAÇÃO COM AUTENTICAÇÃO (https)

Tor
HTTPS

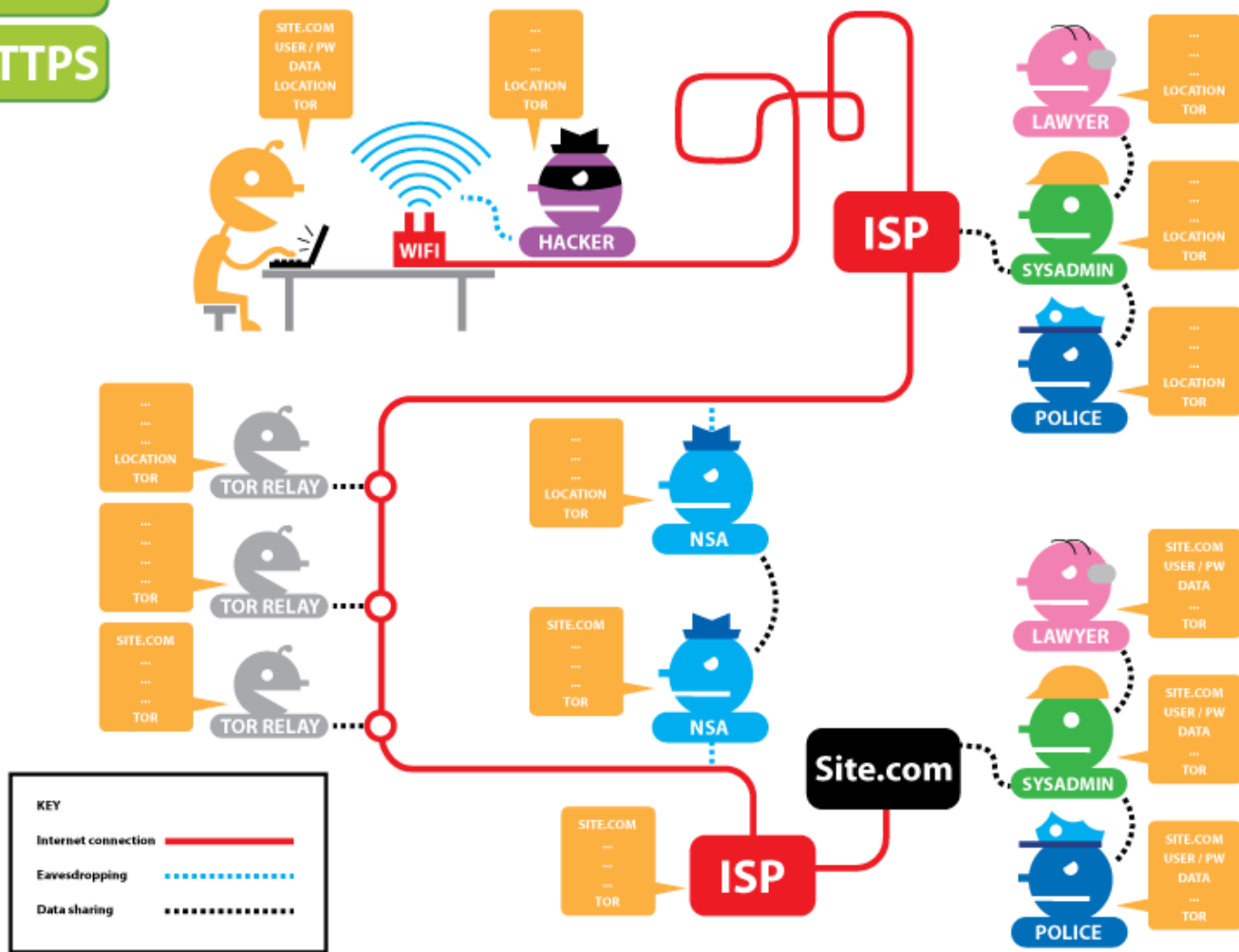


TOR - NAVEGAÇÃO COM ANONIMIA (TOR)



TOR - NAVEGAÇÃO ANONIMA (TOR+HTTPS)

Tor
HTTPS



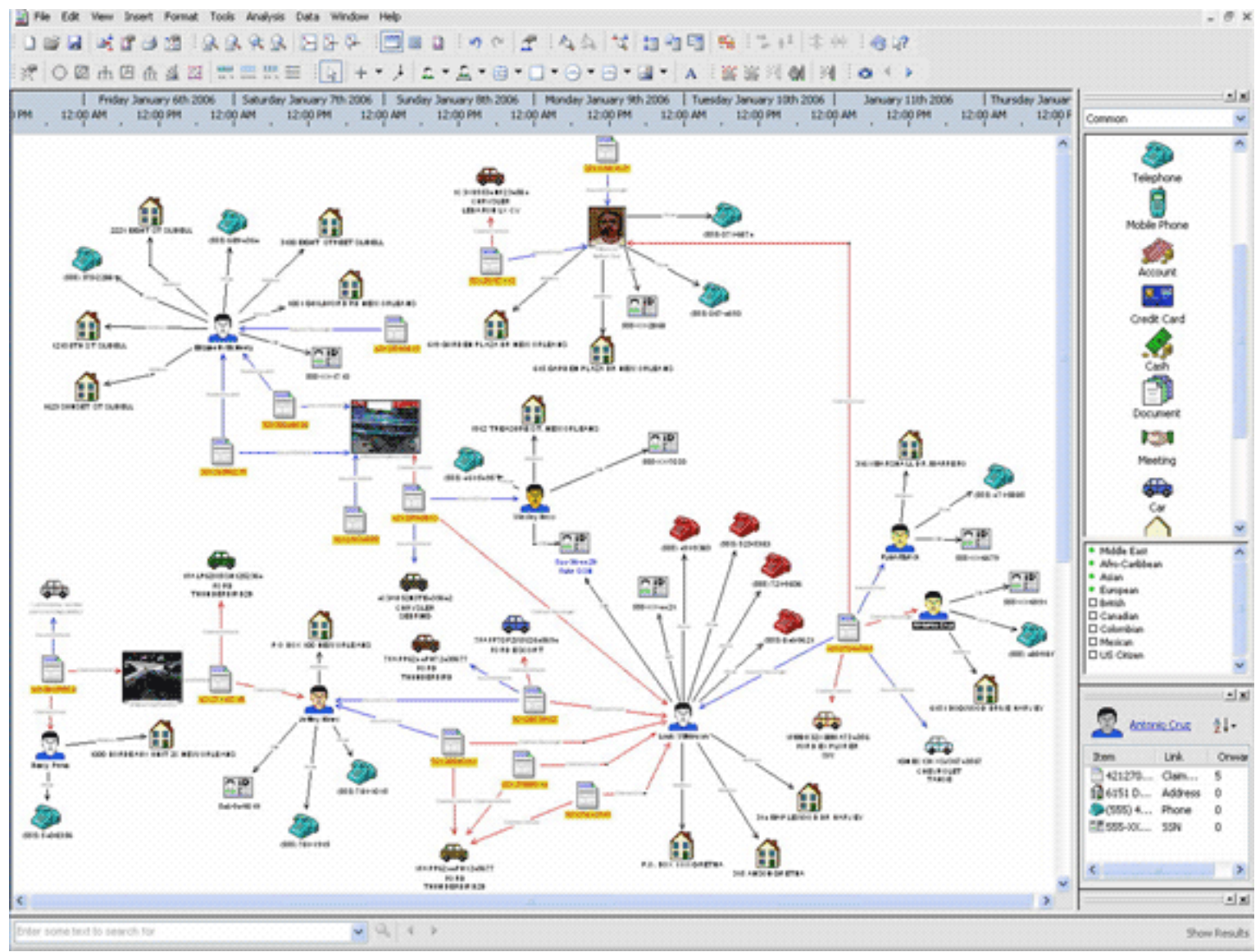
<https://www.eff.org/pages/tor-and-https>



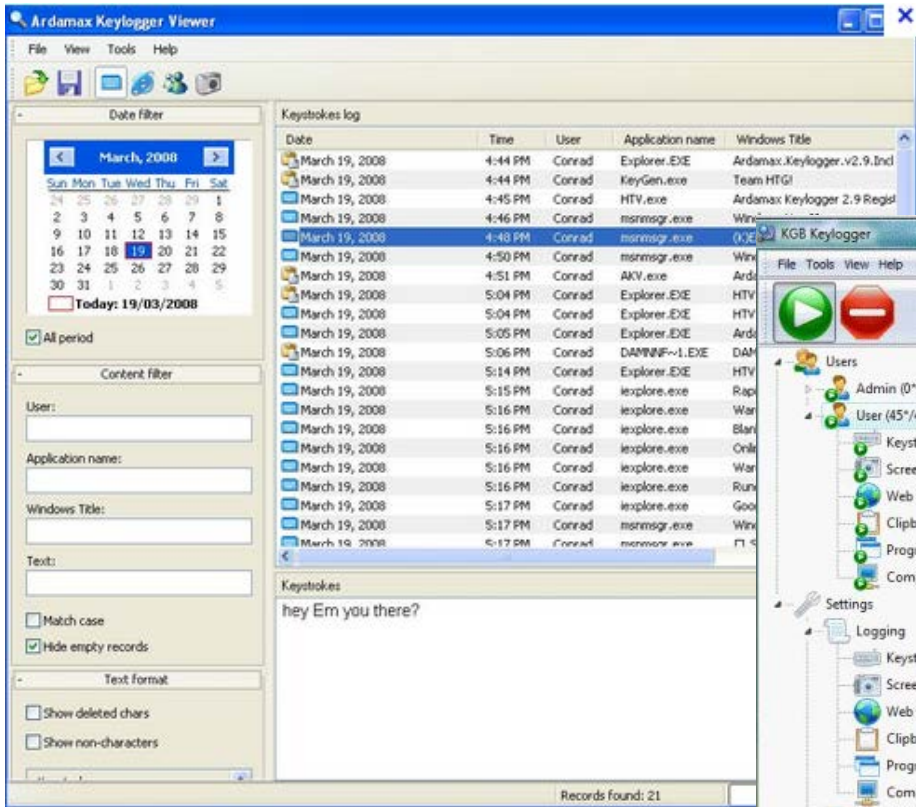
CONTRA INTELIGENCIA

Dados – Informação – Conhecimento – Sabedoria

CORRELACIONAMENTO DE EVENTOS I2



Encase - KEYLOGGER - Ardamax - KGB



Ardamax Keylogger Viewer

File View Tools Help

Date filter: March, 2008

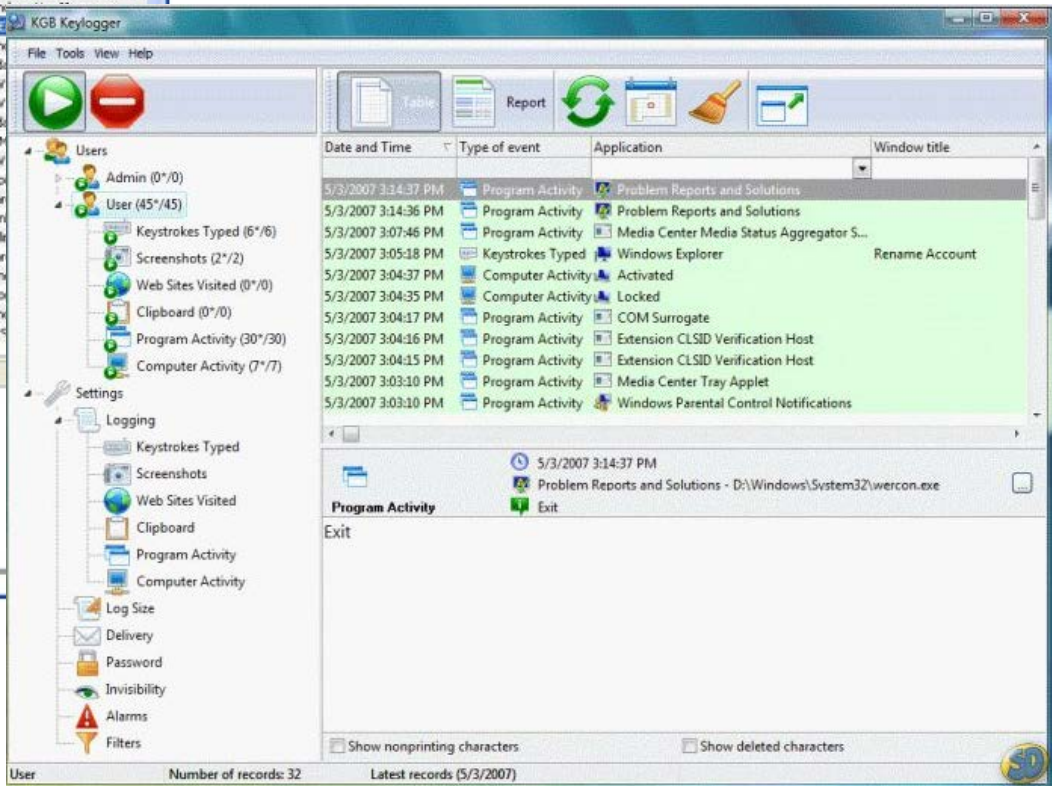
Content filter: User, Application name, Windows Title, Text

Keystrokes log table:

Date	Time	User	Application name	Windows Title
March 19, 2008	4:44 PM	Conrad	Explorer.EXE	Ardamax.Keylogger.v2.9.Incl
March 19, 2008	4:44 PM	Conrad	KeyGen.exe	Team HTGI
March 19, 2008	4:45 PM	Conrad	HTV.exe	Ardamax Keylogger 2.9 Regis
March 19, 2008	4:46 PM	Conrad	msnmsgr.exe	Win...
March 19, 2008	4:48 PM	Conrad	msnmsgr.exe	(J)
March 19, 2008	4:50 PM	Conrad	msnmsgr.exe	Win...
March 19, 2008	4:51 PM	Conrad	AKV.exe	Ard...
March 19, 2008	5:04 PM	Conrad	Explorer.EXE	HTV
March 19, 2008	5:04 PM	Conrad	Explorer.EXE	HTV
March 19, 2008	5:05 PM	Conrad	Explorer.EXE	Ard...
March 19, 2008	5:06 PM	Conrad	DAMNMF-1.EXE	DAM...
March 19, 2008	5:14 PM	Conrad	Explorer.EXE	HTV
March 19, 2008	5:15 PM	Conrad	ieexplore.exe	Rap...
March 19, 2008	5:16 PM	Conrad	ieexplore.exe	War...
March 19, 2008	5:16 PM	Conrad	ieexplore.exe	Blar...
March 19, 2008	5:16 PM	Conrad	ieexplore.exe	Onli...
March 19, 2008	5:16 PM	Conrad	ieexplore.exe	War...
March 19, 2008	5:16 PM	Conrad	ieexplore.exe	Run...
March 19, 2008	5:17 PM	Conrad	ieexplore.exe	Go...
March 19, 2008	5:17 PM	Conrad	msnmsgr.exe	Win...
March 19, 2008	5:17 PM	Conrad	msnmsgr.exe	HTV

Keystrokes: hey Em you there?

Records found: 21



KGB Keylogger

File Tools View Help

Users: Admin (0*/0), User (45*/45)

- Keystrokes Typed (6*/6)
- Screenshots (2*/2)
- Web Sites Visited (0*/0)
- Clipboard (0*/0)
- Program Activity (30*/30)
- Computer Activity (7*/7)

Settings: Logging, Log Size, Delivery, Password, Invisibility, Alarms, Filters

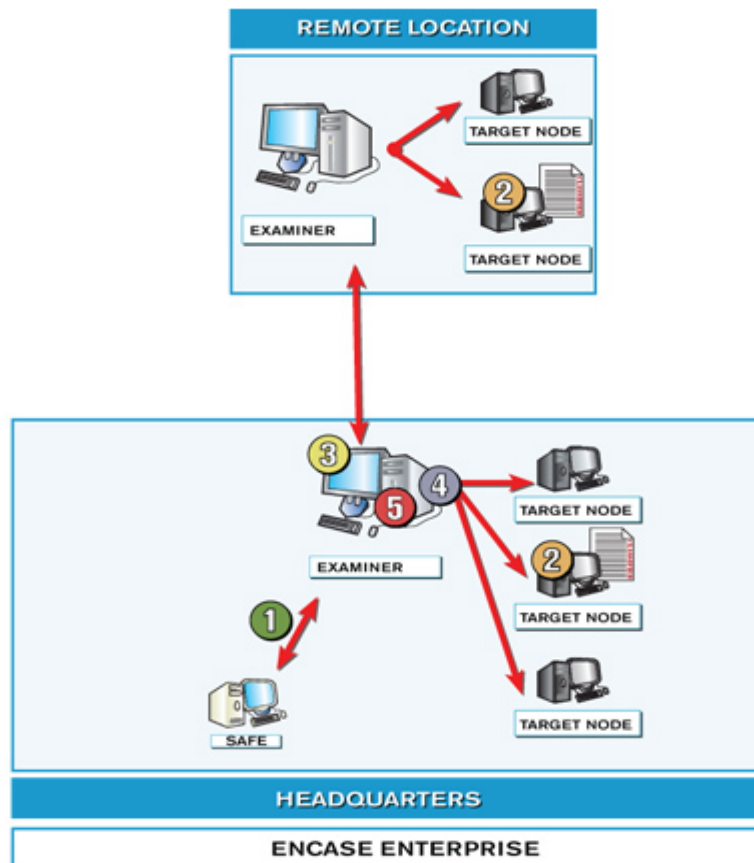
Date and Time	Type of event	Application	Window title
5/3/2007 3:14:37 PM	Program Activity	Problem Reports and Solutions	
5/3/2007 3:14:36 PM	Program Activity	Problem Reports and Solutions	
5/3/2007 3:07:46 PM	Program Activity	Media Center Media Status Aggregator S...	
5/3/2007 3:05:18 PM	Keystrokes Typed	Windows Explorer	Rename Account
5/3/2007 3:04:37 PM	Computer Activity	Activated	
5/3/2007 3:04:35 PM	Computer Activity	Locked	
5/3/2007 3:04:17 PM	Program Activity	COM Surrogate	
5/3/2007 3:04:16 PM	Program Activity	Extension CLSID Verification Host	
5/3/2007 3:04:15 PM	Program Activity	Extension CLSID Verification Host	
5/3/2007 3:03:10 PM	Program Activity	Media Center Tray Applet	
5/3/2007 3:03:10 PM	Program Activity	Windows Parental Control Notifications	

Program Activity: Exit

Show nonprinting characters Show deleted characters

User: Number of records: 32 Latest records (5/3/2007)

Encase Enterprise



- 1** Examiner logs into safe for authentication and authorization
- 2** Examiner sends request to target node to snapshot volatile data or to preview drive
- 3** Examiner analyzes/reviews forensic or volatile data from target node
- 4** Analyze further or acquire image
- 5** Generate reports



Welcome : segurancadainformacao@menospapel.com.br



Home



My Computer



My Logs



Download



My Account



Support



Logout

LOG VIEWERS

Live Control Panel

Top 10 Reports

Screenshot Logs

Keystroke Logs

Website Logs

Application Logs

File/Folder Change Logs

Clipboard Logs

User PC Activity Logs

Website Logs

Application Logs

File/Folder Change Logs

Clipboard Logs

User PC Activity Logs

Instant Messenger Logs

Facebook Logs

MySpace Logs

Profanity Alert Logs

Mic Recording Logs

FILTERING

Application Filtering

Chat Messenger Filtering

Website Filtering

Social Network Filtering

Time Control

USER TOOLS

Browse Uploaded Files

View Remote Location

Location Logs

Lists approximate locations and IP addresses of the remote computer.

Show Specific User:



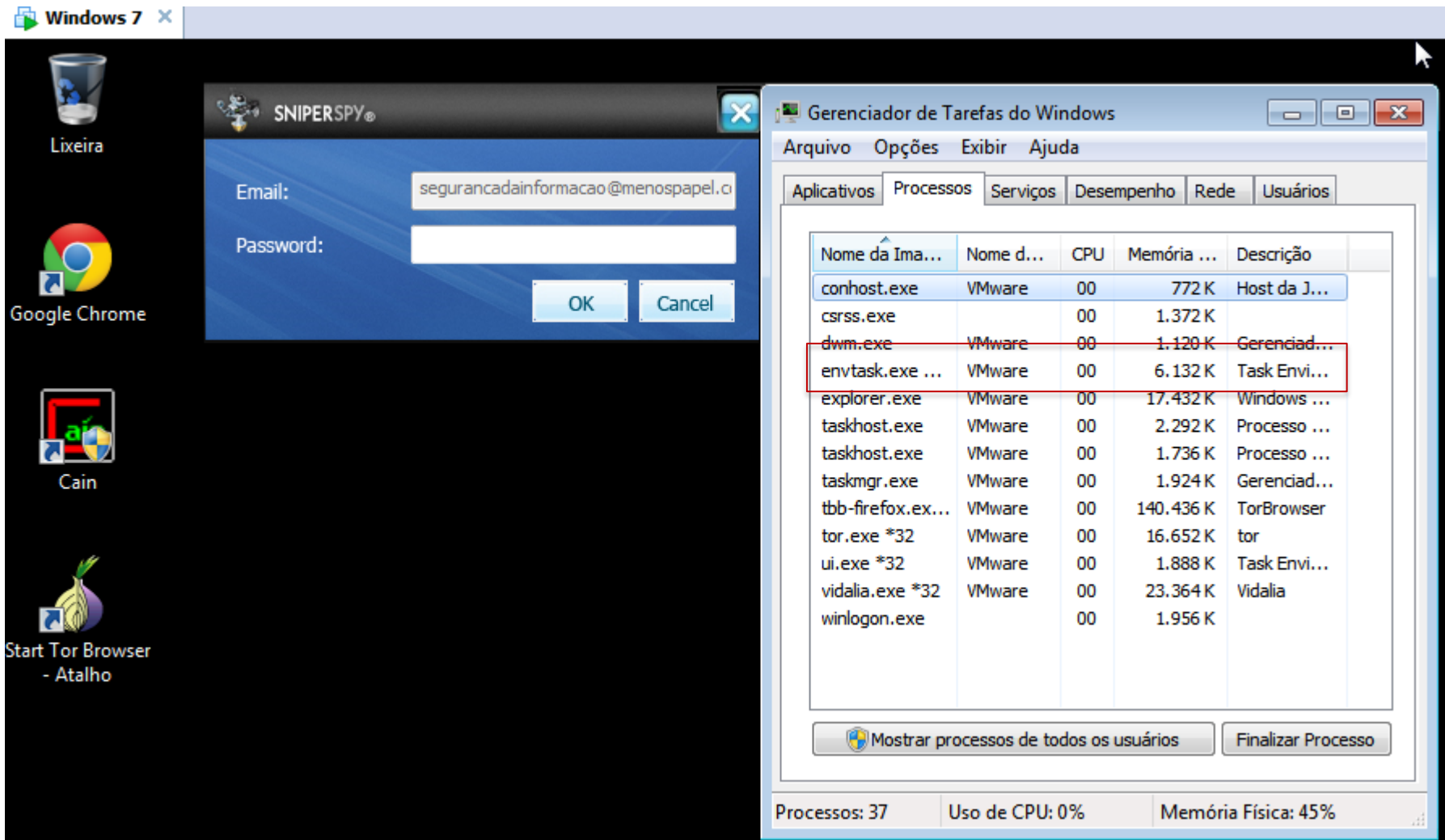
	TIME	IP ADDRESS	COUNTRY	REGION	CITY	LATITUDE	LONGITUDE	USERNAME@COMPUTER	View Map
<input type="checkbox"/>	2013-08-22 19:58:38	177.132.6.52	BRAZIL	PARANA	CURITIBA	-25.4278	-49.2731	VMware@VMWARE-PC	
<input type="checkbox"/>	2013-08-21 17:09:59	201.68.244.92	BRAZIL	SAO PAULO	SAO PAULO	-23.5475	-46.6361	VMware@VMWARE-PC	

Select All | Delete Selected | Delete All

Showing 1 - 2 of 2 records

<input type="checkbox"/>	2013-08-22 23:59:13							VMware@VMWARE-PC	
		[LEFT CTRL]v							
<input type="checkbox"/>	2013-08-22 23:59:13							VMware@VMWARE-PC	
		99[LEFT SHIFT]sn00m[LEFT SHIFT]p33							
<input type="checkbox"/>	2013-08-22 23:58:52	Program Manager						VMware@VMWARE-PC	
		[LEFT CTRL][LEFT CTRL][LEFT CTRL][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT]m							
<input type="checkbox"/>	2013-08-21 21:12:22	C:\Windows\system32\CMD.exe						VMware@VMWARE-PC	
		IPCONFIG[ENTER]							
<input type="checkbox"/>	2013-08-21 21:12:07	Menu Iniciar						VMware@VMWARE-PC	
		CALM[BACKSPACE][BACKSPACE][BACKSPACE]DM[BACKSPACE][BACKSPACE]MD[ENTER]							
<input type="checkbox"/>	2013-08-21 21:09:56							VMware@VMWARE-PC	
		[LEFT CTRL][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT][LEFT SHIFT]M							
<input type="checkbox"/>	2013-08-21 18:46:56	SniperSpy Live Control Panel - Google Chrome						VMware@VMWARE-PC	
		[DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN]							
<input type="checkbox"/>	2013-08-21 18:46:56	SniperSpy Live Control Panel - Google Chrome						VMware@VMWARE-PC	

MONITORAMENTO EM TEMPO REAL -



The screenshot displays a Windows 7 desktop environment. On the left, the taskbar includes icons for 'Lixeira', 'Google Chrome', 'Cain', and 'Start Tor Browser - Atalho'. In the center, a 'SNIPERSPY' login dialog box is open, with the email field containing 'segurancadainformacao@menospapel.c' and 'OK' and 'Cancel' buttons. On the right, the 'Gerenciador de Tarefas do Windows' (Task Manager) is open, showing the 'Processos' (Processes) tab. A red box highlights the 'dwm.exe' and 'envtask.exe ...' processes. The status bar at the bottom of Task Manager shows 'Processos: 37', 'Uso de CPU: 0%', and 'Memória Física: 45%'.

Nome da Imagem	Nome do processo	CPU	Memória	Descrição
conhost.exe	VMware	00	772 K	Host da J...
csrss.exe		00	1.372 K	
dwm.exe	VMware	00	1.120 K	Gerenciad...
envtask.exe ...	VMware	00	6.132 K	Task Envi...
explorer.exe	VMware	00	17.432 K	Windows ...
taskhost.exe	VMware	00	2.292 K	Processo ...
taskhost.exe	VMware	00	1.736 K	Processo ...
taskmgr.exe	VMware	00	1.924 K	Gerenciad...
tbb-firefox.ex...	VMware	00	140.436 K	TorBrowser
tor.exe *32	VMware	00	16.652 K	tor
ui.exe *32	VMware	00	1.888 K	Task Envi...
vidalia.exe *32	VMware	00	23.364 K	Vidalia
winlogon.exe		00	1.956 K	

TOPSY

Search and Analyze the Social Web.

EVERYTHING LINKS TWEETS PHOTOS VIDEOS INFLUENCERS

@erasmoguilmaeres

TOPSY

@erasmoguilmaeres



Ordenar por relevância



Últimos Resultados

Passado 1 Hora 0

Passado 1 dia 0

Passados sete dias

Passados 30 dias 0

All Time 0

Gama específica

Tudo

Ligações

Tweets

Fotos

Vídeos

Influenciadores

Todos Idiomas

Inglês

BitDefender Lança varredura anti-malware parágrafo Twitter - Segurança - IDG Now!

idgnow.uol.com.br/seguranca/2011/09/06/bitdefender-lanca-scan-anti-malware-para-twitter



José Luiz Goldfarb @jgoldfarb

RT @ ErasmoGuimaraes: BitDefender Lança varredura anti-malware parágrafo Twitter ## malwares Twitter <http://t.co/8BPPV9n> via @IDGNow

2 anos atrás Responder Retweeter Favorito 22 mais



Coriolano Camargo @ coriolanoac

@ ErasmoGuimaraes: Manifestações racistas e homofóbicas na internet PODEM sofrer punições Legais | prof @ coriolanoAC <http://ning.it/mH9mVv>

2 anos atrás Responder Retweeter Favorito 5 mais



Val Ce @ val_ce

@ Jorgewcosta igsau de @ @ @ LincolnWerneck CoriolanoAC alvaresotero @ @ @ cossovincius ErasmoGuimaraes @ fernando_de_pb @ LeandroDBCcenter # BoaNoite

3 anos atrás Responder Retweeter Favorito 2 mais

[CRIMES DE INFORMÁTICA] Condutas No Mundo virtuais exigem Legislação Específica. Saiba Mais em:

sociedadeainformacao.ning.com/forum/topics/crimes-de-informatica-Condutas?xg_source=shorten_twitter



Emerson Wendt @ emersonwendt

RT @ ErasmoGuimaraes: [CRIMES DE INFORMÁTICA] Condutas No Mundo virtuais exigem Legislação Específica. Saiba Mais em: <http://ning.it/fulgOp>

3 anos atrás Responder Retweeter Favorito 8 mais



Lisandra Golba @ @Joelha

FACEBOOK - TRACERT

facebook



Olá Erasmo,

Detectamos um login em sua conta de um dispositivo não reconhecido às Sexta, 23 de agosto de 2013 às 01:10.

Sistema operacional: Windows 8

Navegador: Firefox

Localização: Curitiba, PR, BR (IP=177.132.6.52)

Sessões ativas

	Sessão atual	Encerrar todas as atividades
	Local: Curitiba, PR, BR (Aproximado)	
	Tipo de dispositivo: Firefox no Windows 8	
Se notar qualquer dispositivo ou local que não lhe é familiar, clique em "Encerrar atividade" para finalizar a sessão.		
Acessado pela última vez:	Ontem às 15:57	Encerrar atividade
	Local: Curitiba, PR, BR (Aproximado)	
	Tipo de dispositivo: Firefox no Windows 8	
Acessado pela última vez:	Ontem às 08:18	Encerrar atividade
	Local: Sao Paulo, SP, BR (Aproximado)	
	Tipo de dispositivo: Facebook for Android no Android 2	
Acessado pela última vez:	20 de agosto às 13:40	Encerrar atividade
	Local: Santos, SP, BR (Aproximado)	
	Tipo de dispositivo: Firefox no Windows 8	
Acessado pela última vez:	1 de agosto às 01:56	Encerrar atividade
	Local: Sao Paulo, SP, BR (Aproximado)	
	Tipo de dispositivo: Firefox no Windows 8	
Acessado pela última vez:	31 de julho às 22:29	Encerrar atividade
	Local: Brasilia, DF, BR (Aproximado)	
	Tipo de dispositivo: Chrome no Windows 8	

: serviços de Internet.

ode estar tentando acessá-la.

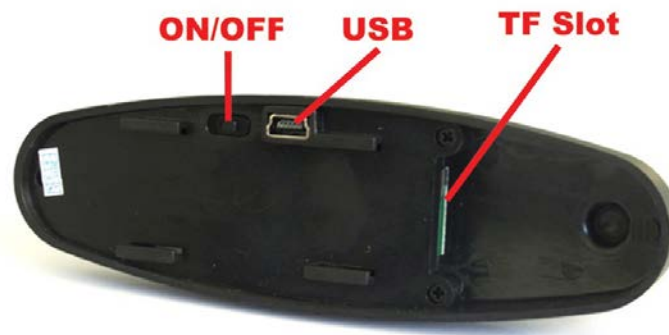
Relógio De Parede Espião Escuta Gsm De Longa Duracao 15 Dias



DISPOSITIVOS ELETRÔNICOS



Cabide Espiao Camera Alta Resolução +detector Movimento +8gb



DISPOSITIVOS ELETRÔNICOS



MINI GPRS



Quadband GSM



GSM/GPRS/GPS



SIM



DISPOSITIVOS ELETRÔNICOS



**FILTRO DE LINHA ESCUTA
ESPIAO COM CAMERA GSM REAL TIME**



KeyGrabber

ClickJuris[®]

Sua central de Inteligência Jurídica.

Serviços

Monitoramento de
Diários Oficiais

Cadastro

 LOGIN

Monitoramento e Alerta de Diários Oficiais

GRÁTIS

Monitore GRATUITAMENTE seu nome e termos de interesse em todos os Diários Oficiais e de Justiça do Brasil e receba Alertas de novos resultados em seu e-mail.



Tweet

eras.com@gmail.com

.....

Carregando...

Mais de
60.000 usuários e
400.000
Termos monitorados


EM TODO


SPYPIG - RASTREAMENTO





SpyPig Classic


SpyPig Factory

step 1 Your email address 



Save 

step 2 Your message title 


step 3 Select your SpyPig tracking image 
or [upload your own image](#)





Four small images of the SpyPig piggy bank are shown in a row. The first is the standard pink piggy bank. The second is a pink piggy bank with a red "X" over its eyes. The third is a grey piggy bank. The fourth is a pink piggy bank with the text "I know you've read my email!" written on its side. Each image has a radio button below it.

step 4  [Click to Create My SpyPig](#) 


You




step 5 Copy & paste the SpyPig image above into your email message.  - Read first to see how!

step 6 Send your email as usual. 
Check also your spam folder for your notification email.

Hands ON

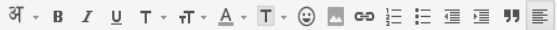
ENVIAR Salvar agora Descartar Rascunho salvo automaticamente em 02:20 (0 minutos atrás) 

Para: 


[Adicionar Cc](#) [Adicionar Cco](#)

Assunto:

[Anexar um arquivo](#) Inserir: [Convite](#)

 [Verificar ortografia](#)

Ola Junior,
Com foi o seu final de semana?




--
Atenciosamente
Eras - [ERGJ](#)

sexta-feira, 16 de dezembro de 2011

◀ dezembro de 2011 ▶

D	S	T	Q	Q	S	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7



02:21:29


Doutorado em Direito - www.iunib.com - Pcls de R\$ 650,00 Aulas Janeiro/Julho na Argentina Qual o motivo deste anúncio?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	mim	Desejo um bom inicio de semana! - Ola Junior, Com foi o seu final de semana? -- Atenciosamente Eras - ERGJ	02:23
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Notification	Your email "Ola voce recebeu um novo IP" has been read 1 time! (self-opened?) - Free email tracking system - Find out when your email has been read by recipient! Visit ..	02:20
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			space 01:17
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			01:15
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			01:04
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			ferta (00:59
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			00:01
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>			23:40
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			23:31
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			22:51
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			22:29

sexta-feira, 16 de dezembro de 2011

◀ dezembro de 2011 ▶

D	S	T	Q	Q	S	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7



02:24:31

i Seu fuso horário atual não é reconhecido. Selecione um fuso horário válido pelo link abaixo.

[Alterar configurações de data e hora...](#)

Email Title: Ola voce recebeu um novo IP

Sent by You: Friday, December 16, 2011, 2:17:59 AM (GMT -2:00)

Your IP Address: 201.26.45.147
(201-26-45-147.dsl.telesp.net.br)

Opened by Recipient: Friday, December 16, 2011, 2:20:02 AM (GMT -2:00)
2 minutes 3 seconds

Your email has been opened **1** time
Up to 5 "opens" are tracked

Recipient Location: Santos, Sao Paulo, Brazil
(May be inaccurate – See notes below)

Recipient IP Address: 201.26.45.147
(201-26-45-147.dsl.telesp.net.br)

Targets Map View

Latitude	Longitude	Time
0.923065	-37.047205	2011-12-14 18:06:08
0.923065	-37.047205	2011-12-13 14:37:06
0.92280972	-37.04751849	2011-12-12 13:18:00
0.924885	-37.08126068	2011-12-07 23:56:38
0.922809	-37.047205	2011-12-05 13:26:24
3.522442	-46.66198349	2011-12-02 12:33:03
0.924885	-37.08126068	2011-11-30 21:31:48
0.99421759	-37.06433545	2011-11-30 16:01:41
0.924885	-37.08126068	2011-11-28 22:00:54
0.92279521	-37.0472813	2011-11-28 20:25:02
0.924885	-37.08126068	2011-11-26 19:52:48
0.924885	-37.08126068	2011-11-26 13:20:58
1.4086473	-37.31796026	2011-11-25 14:12:44
0.855674	-37.123611	2011-11-22 14:30:42
0.964179	-37.05403	2011-11-19 16:25:58
0.92437935	-37.04521179	2011-11-18 19:32:44
1.00012	-37.06875	2011-11-06 16:12:53
0.94906045	-37.07229137	2011-11-03 21:33:56
0.9095421	-37.0747732	2011-10-28 19:34:04
0.924885	-37.08126068	2011-10-26 19:53:12

9 check in
de 26/10/2011

a

14/12/2011



Information retrieved from twitter.

weet was : Dia de prova é aquele silêncio... (@ Faculdade Pio Décimo w/ 2 others) [pic]: <http://t.co/rBW4oLoB>
<https://twitter.com/joaopereira1000/status/141992851906113537>

Rastreamento de Check-in na web

Latitude	Longitude	Time
10.923065	-37.047205	2011-12-14 18:06:08
10.923065	-37.047205	2011-12-13 14:37:06
10.92280972	-37.04751849	2011-12-12 13:18:00
10.924885	-37.08126068	2011-12-07 23:56:38
10.922809	-37.047205	2011-12-05 13:26:24
23.522442	-46.66198349	2011-12-02 12:33:03
10.924885	-37.08126068	2011-11-30 21:31:48
10.99421759	-37.06433545	2011-11-30 16:01:41
10.924885	-37.08126068	2011-11-28 22:00:54
10.92279521	-37.0472813	2011-11-28 20:25:02
10.924885	-37.08126068	2011-11-26 19:52:48
10.924885	-37.08126068	2011-11-26 13:20:58
11.4086473	-37.31796026	2011-11-25 14:12:44
10.855674	-37.123611	2011-11-22 14:30:42
10.964179	-37.05403	2011-11-19 16:25:58
10.92437935	-37.04521179	2011-11-18 19:32:44
11.00012	-37.06875	2011-11-06 16:12:53
10.94906045	-37.07229137	2011-11-03 21:33:56
10.9095421	-37.0747732	2011-10-28 19:34:04
10.924885	-37.08126068	2011-10-26 19:53:12



quinta-feira, 15 de dezembro de 2011

de dezembro de 2011

D	S	T	Q	Q	S	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7



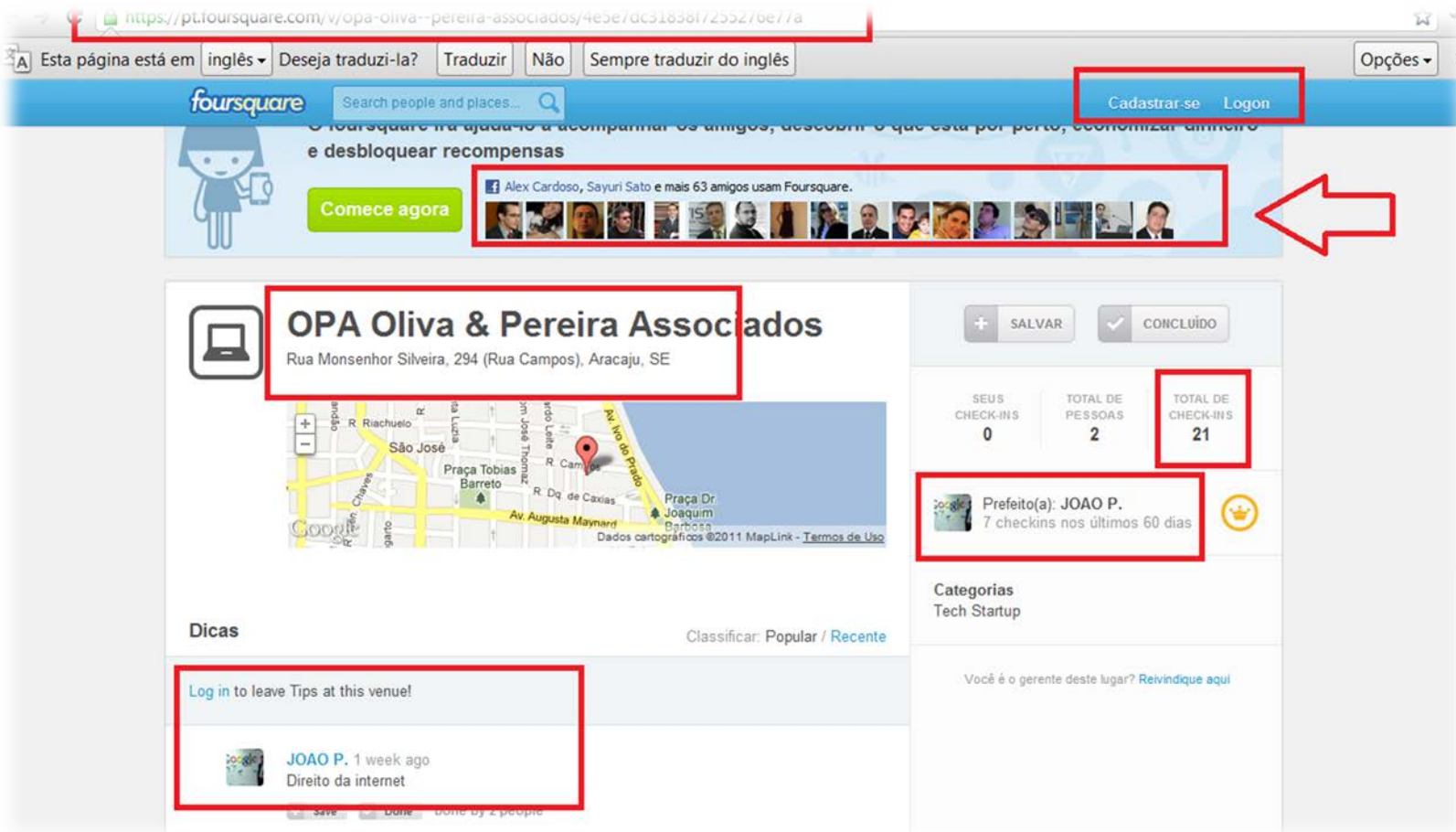
01:16:54

Seu fuso horário atual não é reconhecido. Selecione um fuso horário válido pelo link abaixo.

[Alterar configurações de data e hora...](#)

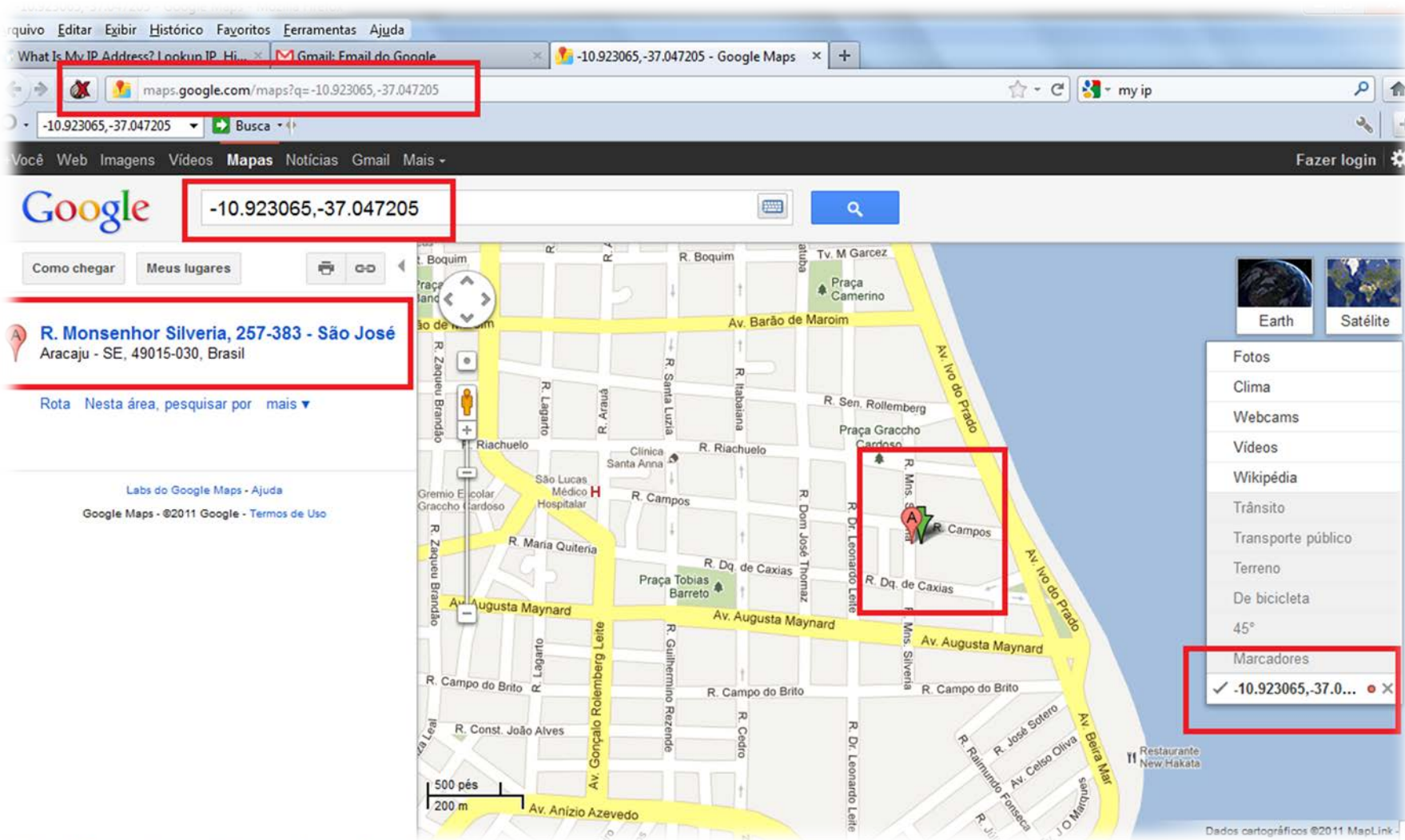
Information retrieved from twitter.
 Tweet was: I'm at OPA Oliva & Pereira Associados w/ @afonso85 <http://t.co/ZtPGh35J>
<https://twitter.com/joaoopereira1000/status/147014524124397569>

Check-in Local? Vale a pena colocar em risco a sua privacidade?



The screenshot shows a Foursquare venue page for "OPA Oliva & Pereira Associados" located at Rua Monsenhor Silveira, 294 (Rua Campos), Aracaju, SE. The page is annotated with several red boxes highlighting specific elements:

- Top Navigation:** A box highlights the "Cadastrar-se" (Sign up) and "Logon" (Log in) buttons.
- User Activity:** A box highlights a notification that "Alex Cardoso, Sayuri Sato e mais 63 amigos usam Foursquare." with a red arrow pointing to it from the right.
- Venue Information:** A box highlights the venue name "OPA Oliva & Pereira Associados" and its address "Rua Monsenhor Silveira, 294 (Rua Campos), Aracaju, SE".
- Map:** A map shows the location of the venue in Aracaju, SE.
- Statistics:** A box highlights the statistics: "SEUS CHECK-INS 0", "TOTAL DE PESSOAS 2", and "TOTAL DE CHECK-INS 21".
- User Profile:** A box highlights the profile of "JOAO P.", who is the "Prefeito(a)" (Mayor) of the venue, with "7 checkins nos últimos 60 dias" (7 check-ins in the last 60 days).
- Categories:** The category "Tech Startup" is visible.
- Management:** A box highlights the text "Você é o gerente deste lugar? Reivindique aqui" (Are you the manager of this place? Reclaim here).
- Tips:** A box highlights a tip from "JOAO P." posted "1 week ago" with the text "Direito da internet".



The screenshot shows a Google Maps interface in a browser. The browser's address bar contains the URL `maps.google.com/maps?q=-10.923065,-37.047205`. The search bar at the top of the map also contains the coordinates `-10.923065,-37.047205`. The map displays a street grid in São José, Aracaju, with a red location pin 'A' marking the address `R. Monsenhor Silveria, 257-383 - São José Aracaju - SE, 49015-030, Brasil`. A sidebar on the right contains a list of services, with the 'Marcadores' (Markers) section expanded to show the current location: `✓ -10.923065,-37.0...`. The map includes a scale bar (500 feet / 200 meters) and a copyright notice for 2011 MapLink.





SEGURANÇA DA INFORMAÇÃO

Dados – Informação – Conhecimento – Sabedoria

Obscuridade – Dial Up



USB + Fax modem habilitado



Analise com frequência os logs de todos dispositivos conectados a USB

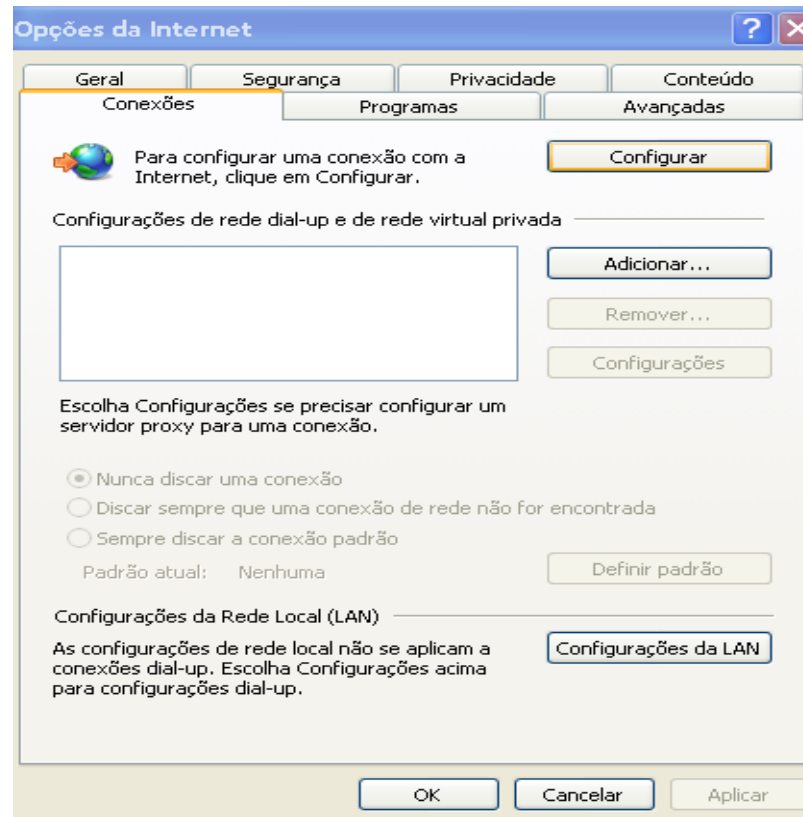
Vulnerabilidades de Hardware



→ FIQUE ATENTO A Dispositivos Moveis - Habilitados

Janela da Oportunidade

Fax Modem
Habilitado permite
“Conexão dial up”



Analise com frequência os logs de todos dispositivos conectados a USB

Vulnerabilidades dos dispositivos móveis

Vazamento de informações sensíveis

1MB >> 1TB

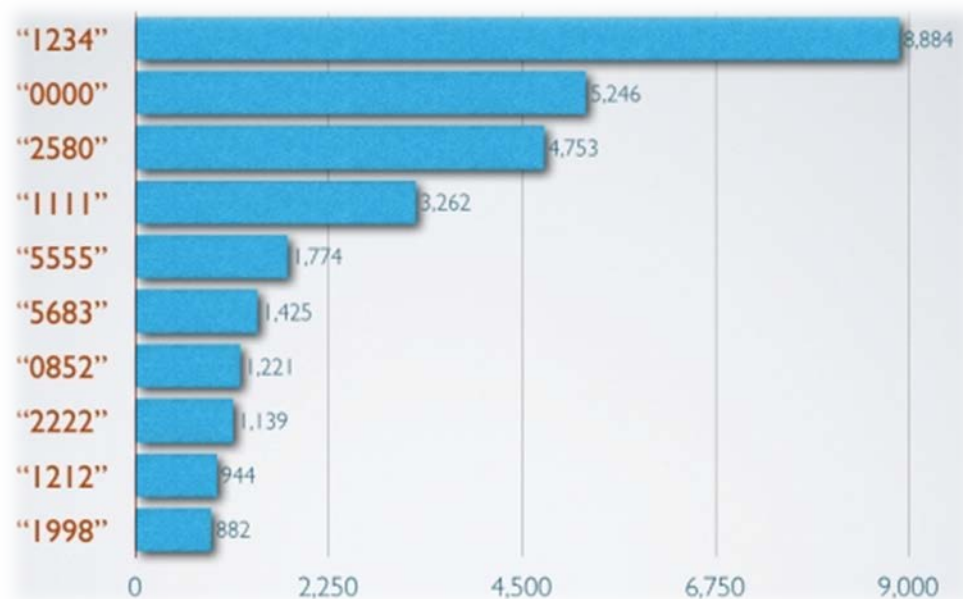
HOJE



Fique atento a estes dispositivos

Vulnerabilidades dos dispositivos móveis

15% de todos os proprietários do iPhone usa uma entre as dez senhas mais comuns



Reflexão: Estas são as 10 senhas mais secretas para iPhone

Vulnerabilidades dos dispositivos móveis

Pendrive - Dispositivos de armazenamento movel - USB



Gestão de ativos

Vulnerabilidades dos dispositivos móveis

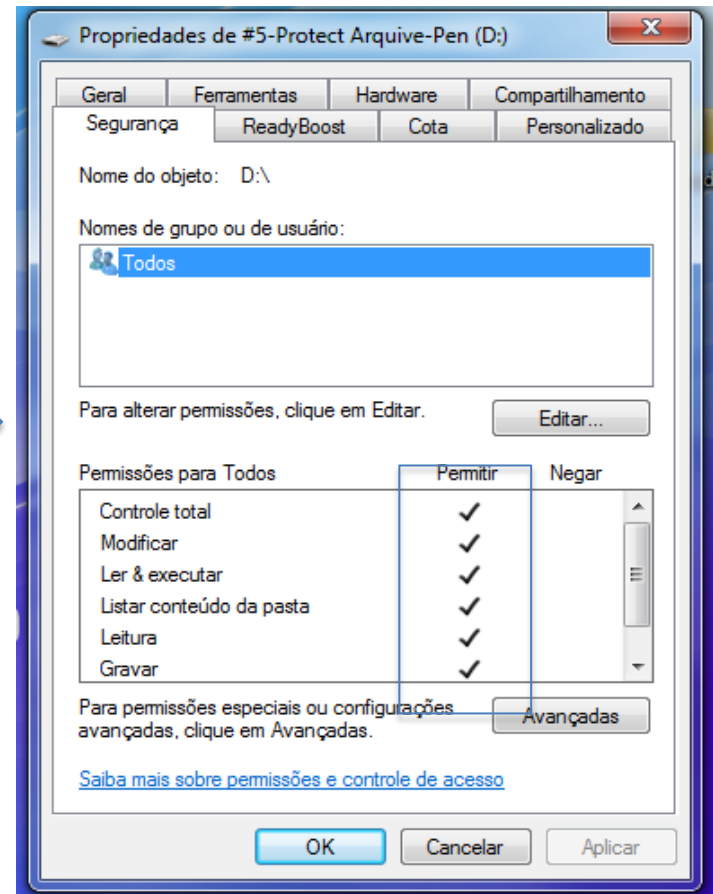
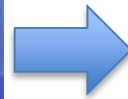
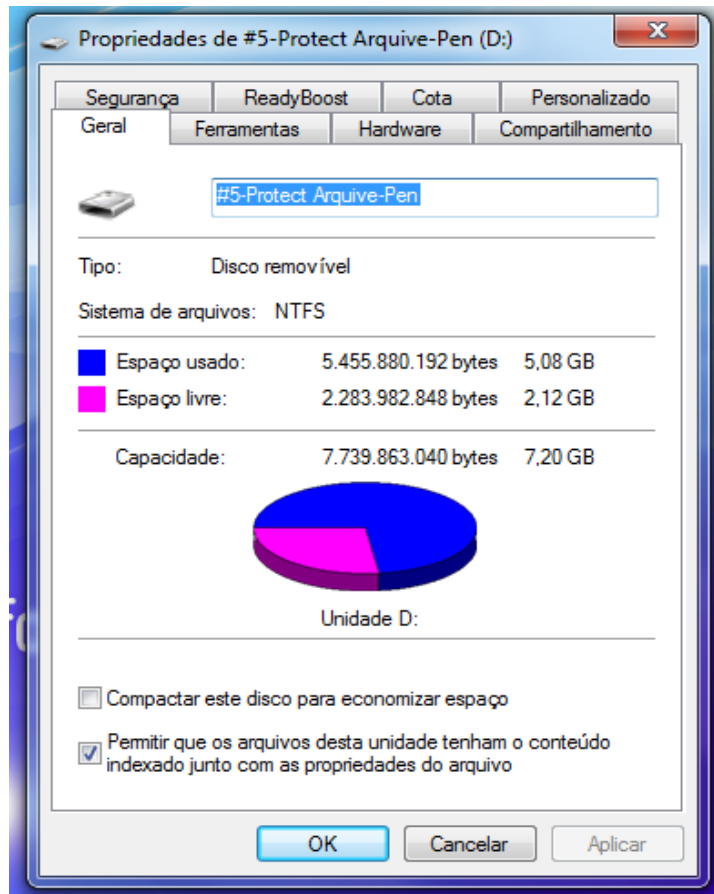
Últimos acessos - Dispositivos moveis - USB

Device Name	Description	Device Type	Connected	Safe To Unpl...
Port_#0001.Hub_#0003	Apple Mobile Device USB Driver	Still Imaging	Yes	Yes
Port_#0001.Hub_#0003	SAMSUNG HD502HI USB Device	Mass Storage	No	Yes
Port_#0001.Hub_#0003	USB 2.0 SD/MMC Reader USB ...	Mass Storage	No	Yes
Port_#0001.Hub_#0003		Mass Storage	No	No
Port_#0001.Hub_#0003	802.11 USB Wireless LAN Card	Vendor Specific	No	No
Port_#0004.Hub_#0006	Kingston DataTraveler 2.0 USB...	Mass Storage	No	Yes

Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Un...
No	No		5b829e1a868a2dc2...	15/12/2011 17:50:26	15/12/2011 20:35:27
No	No		150628599FFF	15/12/2011 17:50:27	15/12/2011 17:50:27
No	No	H:	812822222789	15/12/2011 17:50:27	15/12/2011 17:50:27
No	No			15/12/2011 17:50:27	15/12/2011 17:50:27
No	No		1.0	15/12/2011 17:50:27	15/12/2011 17:50:27
No	No		5B75119B05FC	15/12/2011 17:50:27	15/12/2011 17:50:27

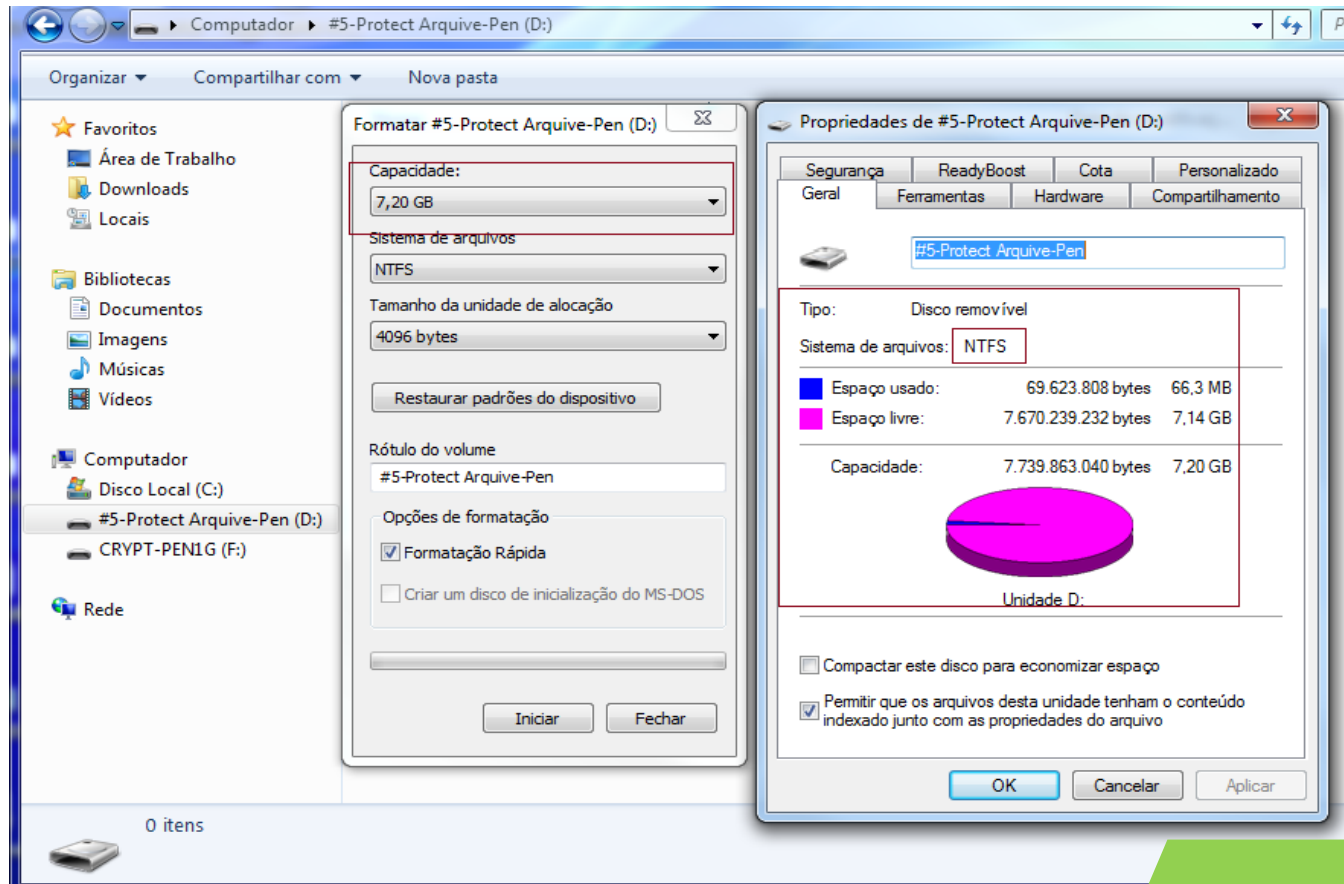
Vulnerabilidades dos dispositivos móveis

NTFS - Permissão e Sistema - Dispositivos moveis - USB



NTFS – FAT32 - exFat

Permissão e Sistema – Formatação # Sanitização



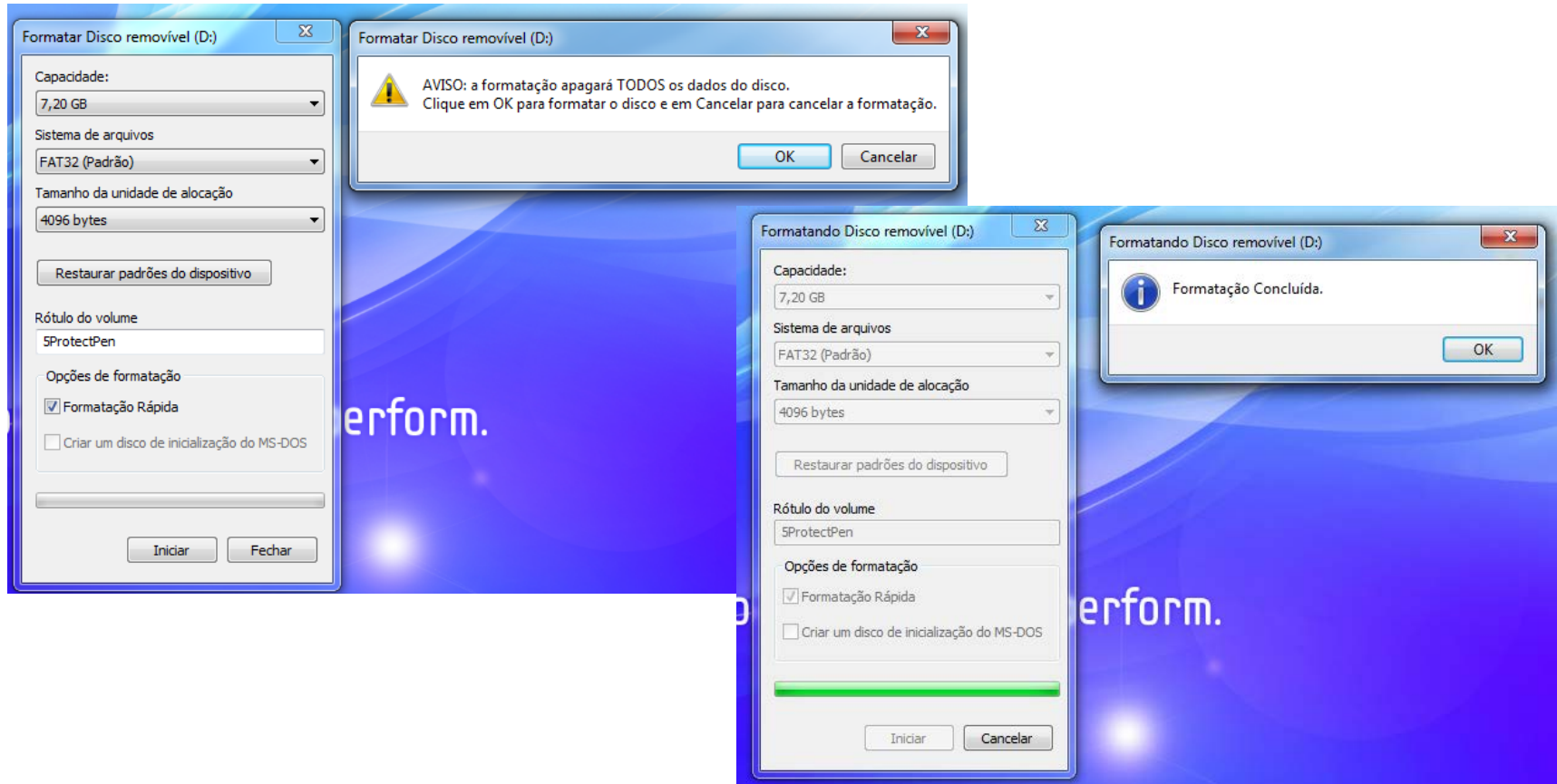
The screenshot displays the Windows File Explorer interface for a removable drive named "#5-Protect Arquivo-Pen (D:)". Two dialog boxes are open over the drive:

- Formatar #5-Protect Arquivo-Pen (D:)**: Shows the drive's capacity as 7,20 GB. The file system is set to NTFS. The allocation unit size is 4096 bytes. The "Formatação Rápida" checkbox is checked.
- Propriedades de #5-Protect Arquivo-Pen (D:)**: Shows the drive as a "Disco removível" with an NTFS file system. It displays a pie chart for disk usage: 66,3 MB (69.623.808 bytes) used and 7,14 GB (7.670.239.232 bytes) free. The total capacity is 7,20 GB (7.739.863.040 bytes). The drive is labeled "Unidade D:".

NTFS

Vulnerabilidades dos dispositivos móveis

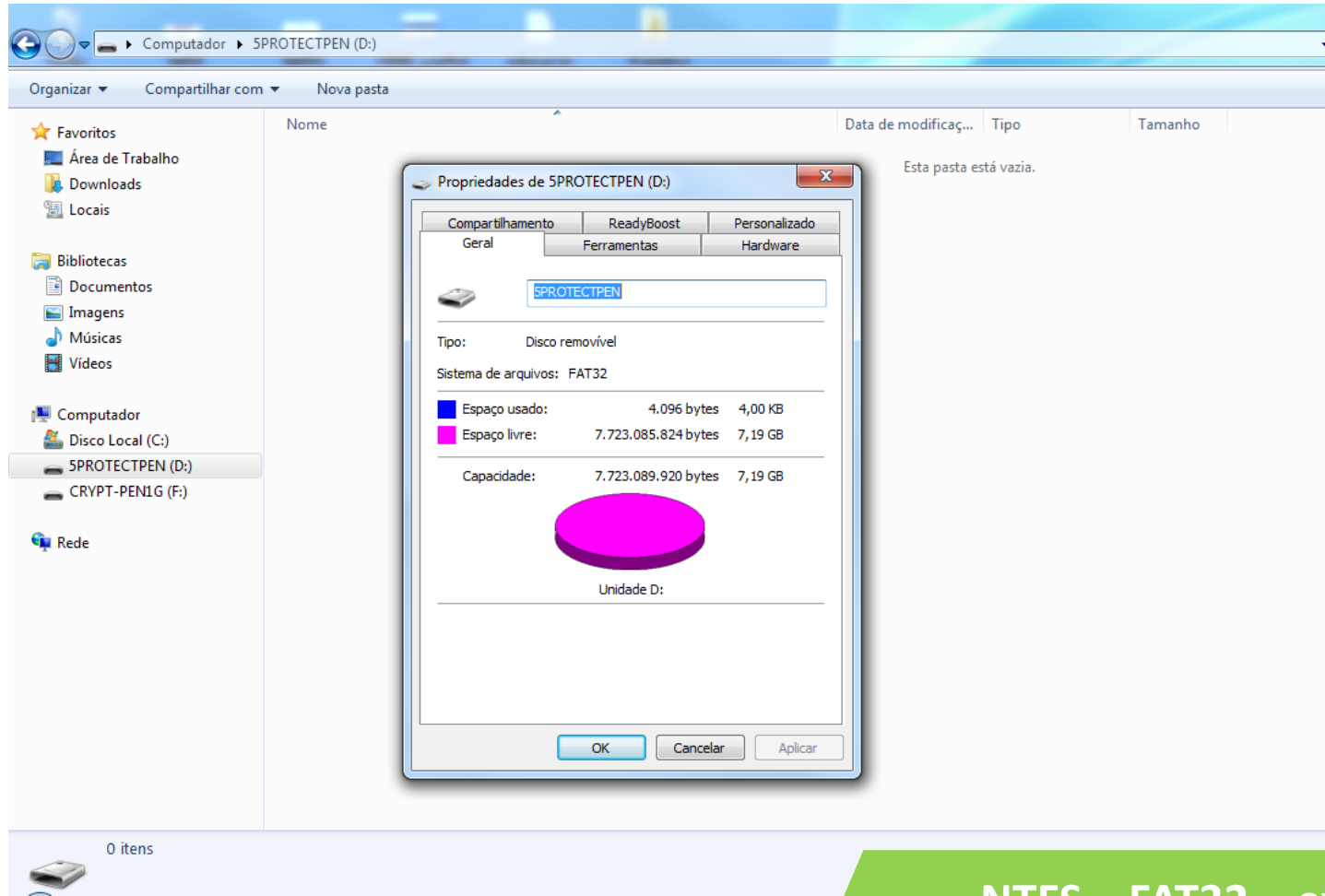
Permissão e Sistema - Dispositivos moveis - USB



NTFS – FAT32 - exFat

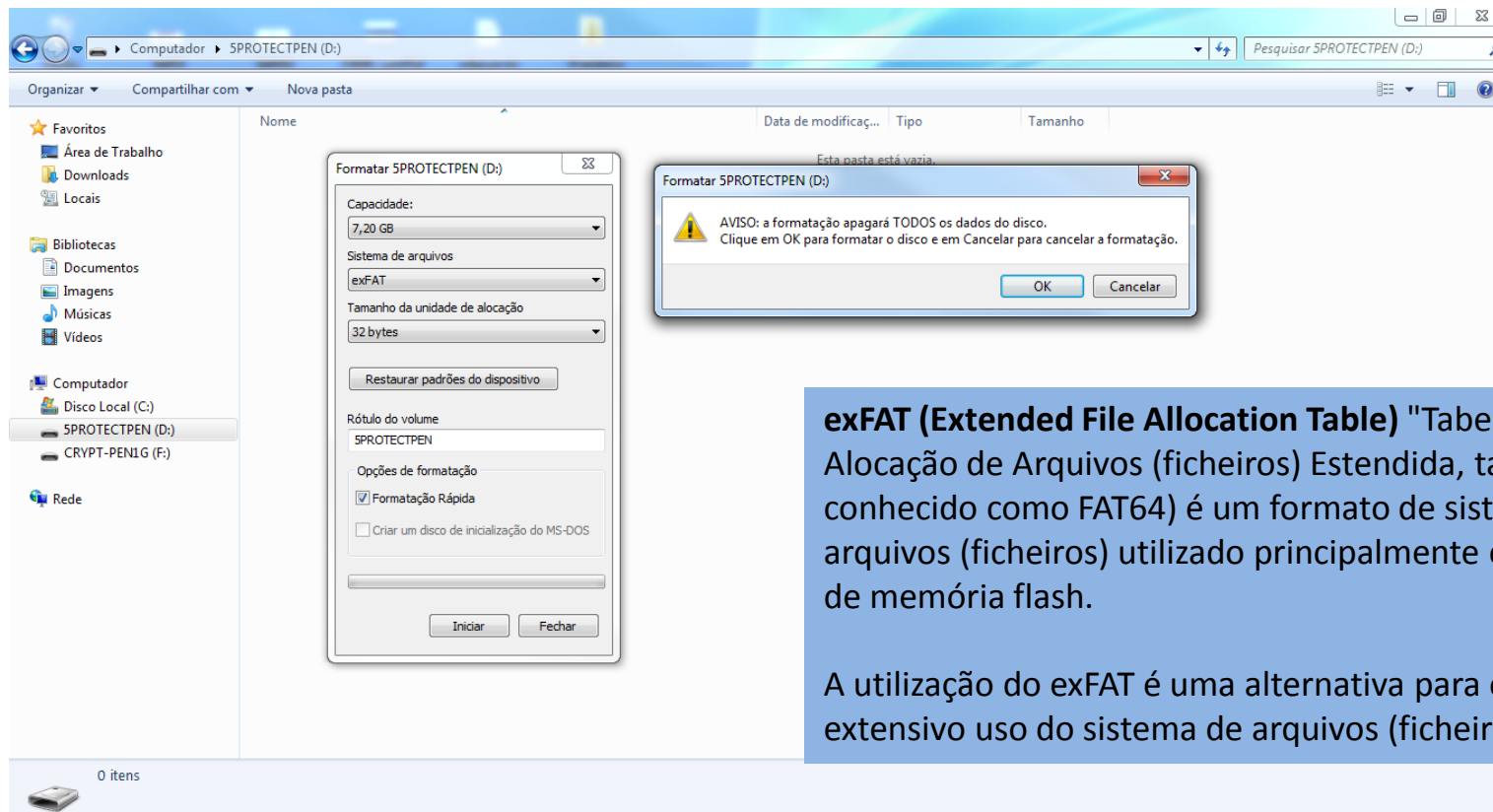
Vulnerabilidades dos dispositivos móveis

Permissão e Sistema - Dispositivos moveis - USB



NTFS – FAT32 - exFat

Permissão e Sistema - Dispositivos moveis - USB



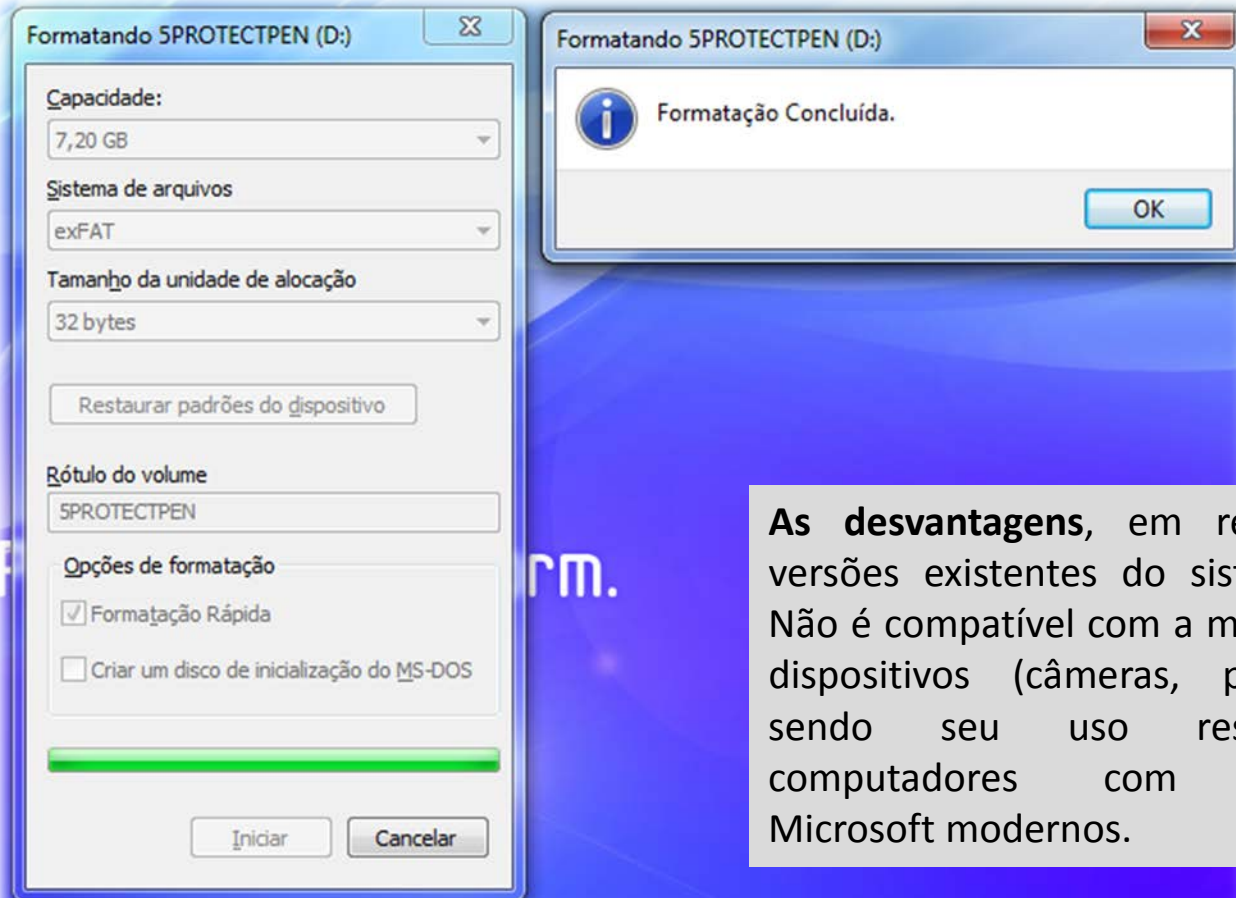
exFAT (Extended File Allocation Table) "Tabela de Alocação de Arquivos (ficheiros) Estendida, também conhecido como FAT64) é um formato de sistema de arquivos (ficheiros) utilizado principalmente em discos de memória flash.

A utilização do exFAT é uma alternativa para evitar o extensivo uso do sistema de arquivos (ficheiros) NTFS.

As desvantagens, em relação às versões existentes do sistema FAT, Não é compatível com a maioria dos dispositivos (câmeras, players,...), sendo seu uso restrito a computadores com sistemas Microsoft modernos.

Vulnerabilidades dos dispositivos móveis

Permissão e Sistema - Dispositivos moveis - USB



As desvantagens, em relação às versões existentes do sistema FAT, Não é compatível com a maioria dos dispositivos (câmeras, players,...), sendo seu uso restrito a computadores com sistemas Microsoft modernos.

Recuperação de arquivos deletado - Dispositivos moveis - USB

Selecione os arquivos que você deseja recuperar marcando as caixas e depois apertando Recuperar.
Para melhores resultados recupere os arquivos em um dispositivo diferente.

<input type="checkbox"/>	Nome do arquivo	Caminho	Última modifica...	Tamanho	Estado	Comentário
<input checked="" type="checkbox"/>	#CSCI013P-2012.doc	D:\?	Desconhecido	9.493 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	#CSCI013P-2012.doc	D:\?	Desconhecido	9.493 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	#CSCI013P-2012.doc	D:\?	Desconhecido	9.486 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	#CSCI013P-2012.doc	D:\?	Desconhecido	9.490 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000001].pdf	D:\?	Desconhecido	2.474.574 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000002].pdf	D:\?	Desconhecido	1.456.678 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input checked="" type="checkbox"/>	[000003].pdf	D:\?	Desconhecido	1.456.490 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input checked="" type="checkbox"/>	[000004].pptx	D:\?	Desconhecido	15.239 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000005].pptx	D:\?	Desconhecido	429 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000006].pdf	D:\?	Desconhecido	1.418.422 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000007].pptx	D:\?	Desconhecido	740 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000008].pdf	D:\?	Desconhecido	659.218 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input checked="" type="checkbox"/>	[000009].pdf	D:\?	Desconhecido	656.786 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000010].pdf	D:\?	Desconhecido	656.526 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000011].pptx	D:\?	Desconhecido	198 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input checked="" type="checkbox"/>	[000012].png	D:\?	Desconhecido	885 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000013].png	D:\?	Desconhecido	266 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000014].png	D:\?	Desconhecido	278 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000015].png	D:\?	Desconhecido	366 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000016].png	D:\?	Desconhecido	269 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000017].png	D:\?	Desconhecido	210 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000018].png	D:\?	Desconhecido	219 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000019].png	D:\?	Desconhecido	161 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000020].png	D:\?	Desconhecido	278 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000021].jpg	D:\?	Desconhecido	229 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000022].png	D:\?	Desconhecido	154 KB	Excelente	Nenhum cluster sobrescrito detectado.
<input type="checkbox"/>	[000023].gif	D:\?	Desconhecido	975 bytes	Excelente	Nenhum cluster sobrescrito detectado.



FAT32, 7,20 GB. Tamanho do cluster: 4096. Found 363 file(s) in 862.06 sec.

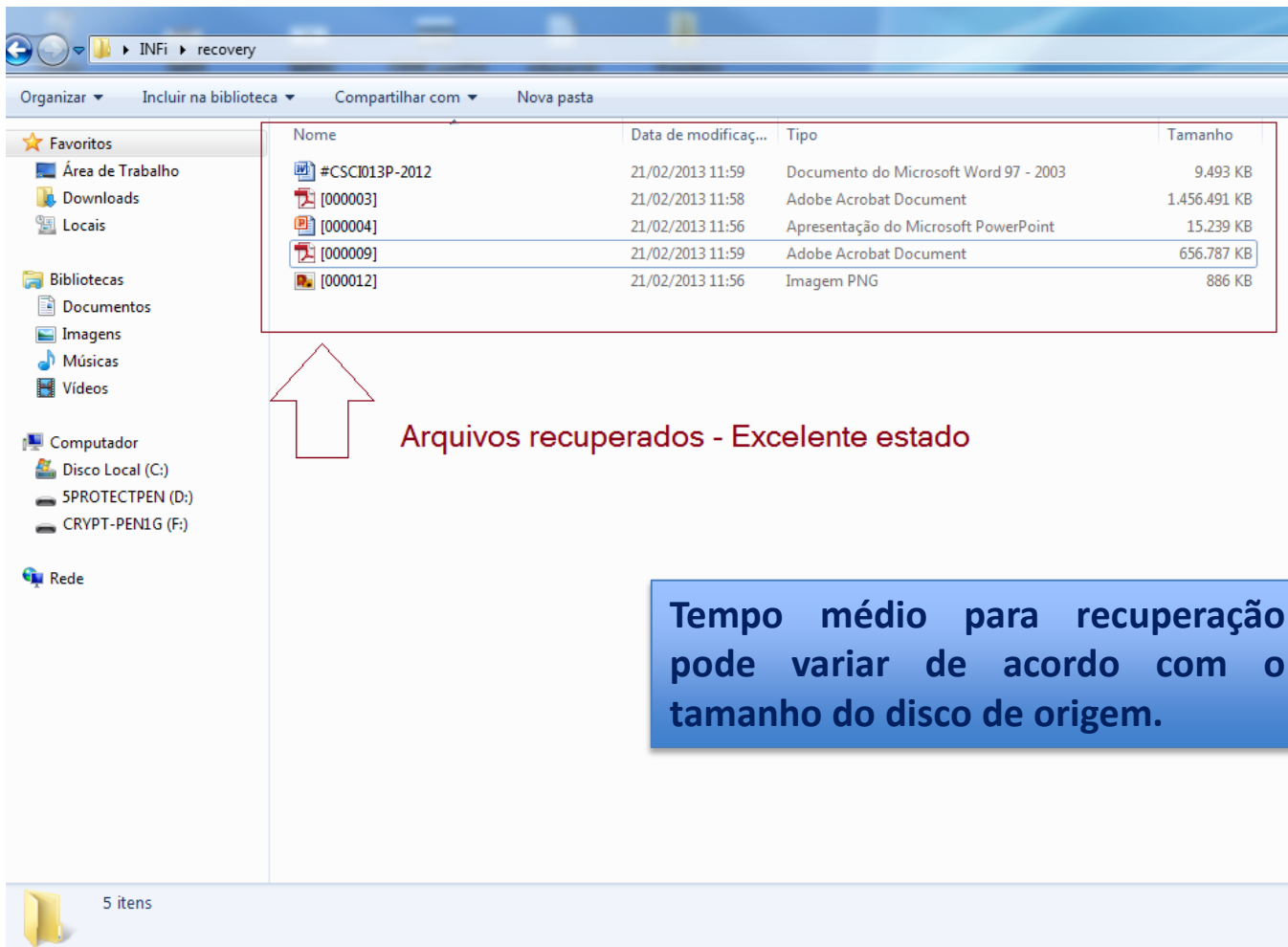
14,36766666666667 Min

363 arquivos

Recomendado a sanitização de discos – Método DOD 5220.22-M
(3 passos)

Vulnerabilidades dos dispositivos móveis

Arquivos recuperados - Dispositivos moveis - USB



The screenshot shows a Windows Explorer window with the address bar set to 'INFI > recovery'. The left sidebar shows the 'Locais' section with drives C:, D:, and F: listed. The main pane displays a table of recovered files:

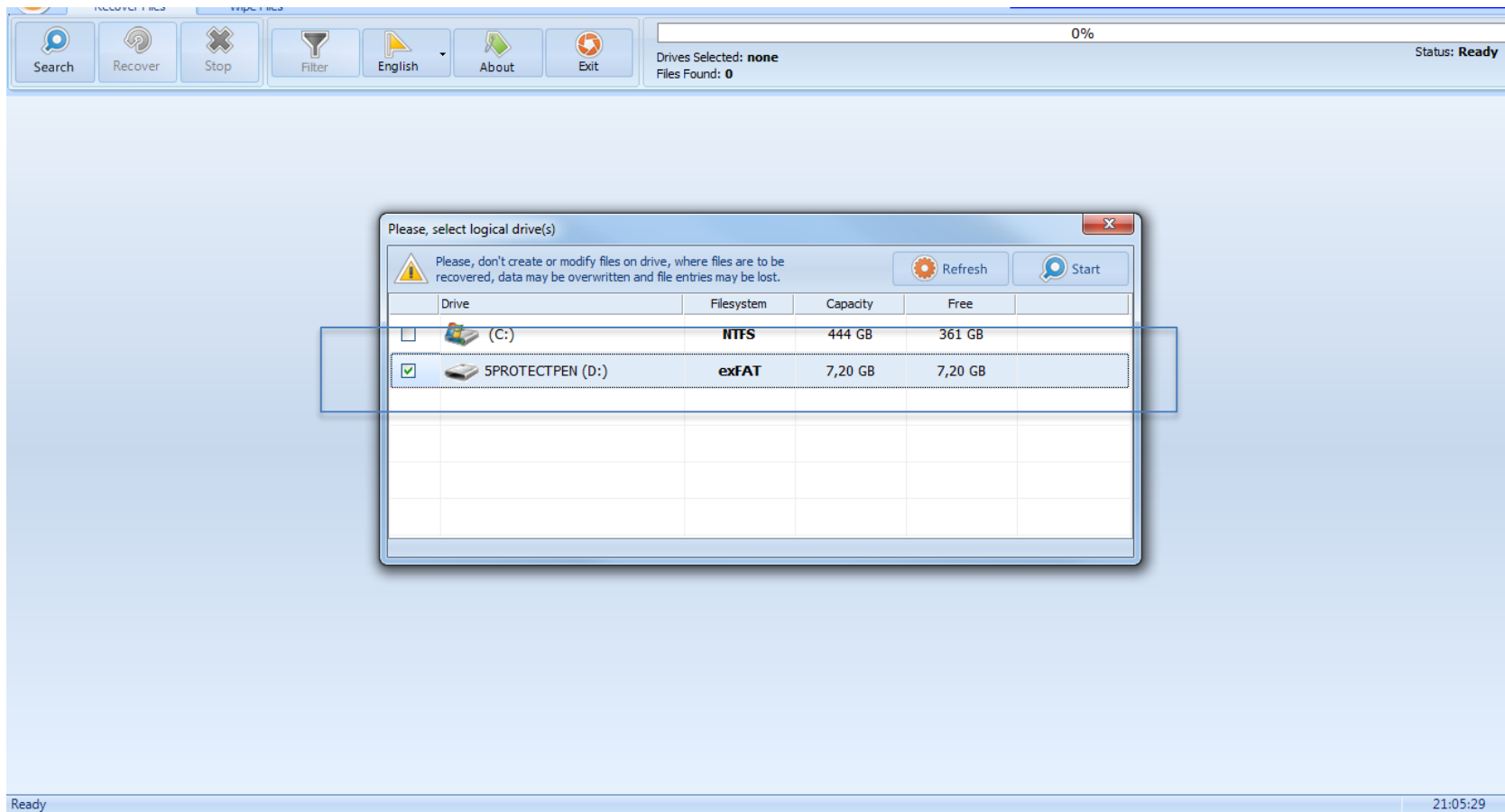
Nome	Data de modificaç...	Tipo	Tamanho
#CSCI013P-2012	21/02/2013 11:59	Documento do Microsoft Word 97 - 2003	9.493 KB
[000003]	21/02/2013 11:58	Adobe Acrobat Document	1.456.491 KB
[000004]	21/02/2013 11:56	Apresentação do Microsoft PowerPoint	15.239 KB
[000009]	21/02/2013 11:59	Adobe Acrobat Document	656.787 KB
[000012]	21/02/2013 11:56	Imagem PNG	886 KB

A red arrow points from the text 'Arquivos recuperados - Excelente estado' to the table. A blue box contains the text: 'Tempo médio para recuperação pode variar de acordo com o tamanho do disco de origem.'

**Recomendado a sanitização de discos – Método DOD 5220.22-M
(3 passos)**

Vulnerabilidades dos dispositivos móveis

Recuperação após a sanitização do Dispositivo móvel - Pendrive



Método DOD 5220.22-M (3 passos)

Vulnerabilidades dos dispositivos móveis

Sanitização de Dispositivo movel – Pendrive 7GB – USB3.0

US DoD 5220.22-M (3 passes)

Status: Start Wipe File System Wizard

0%

List of Folders and Files to be Wiped

Name	Type	Size	Modified	Attr	Full Path
------	------	------	----------	------	-----------

Wipe all previously deleted files

Wiping free space can take a substantial amount of time

Stop Start

wipe directory entries

wipe cluster tips

free disk space with MFT

SPROTECTPEN (D:) - exFAT

Status: Ready

0%

quinta-feira, 21 de fevereiro de 2013

fevereiro de 2013

D	S	T	Q	Q	S	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

21:20:19

O Horário de Verão terminou em domingo, 17 de fevereiro de 2013 às 00:00. O relógio foi retrocedido 1 hora nesse momento.

Alterar configurações de data e hora...

Tempo médio para sanitização de um pendriver com capacidade de 7GB é de aproximadamente 1 hora (dependendo da interface e processamento) USB 3.0 = 57:53,6 seg

Método DOD 5220.22-M (3 passos)

Vulnerabilidades dos dispositivos móveis

Sanitização de Dispositivo movel – Pendrive – USB 2.0

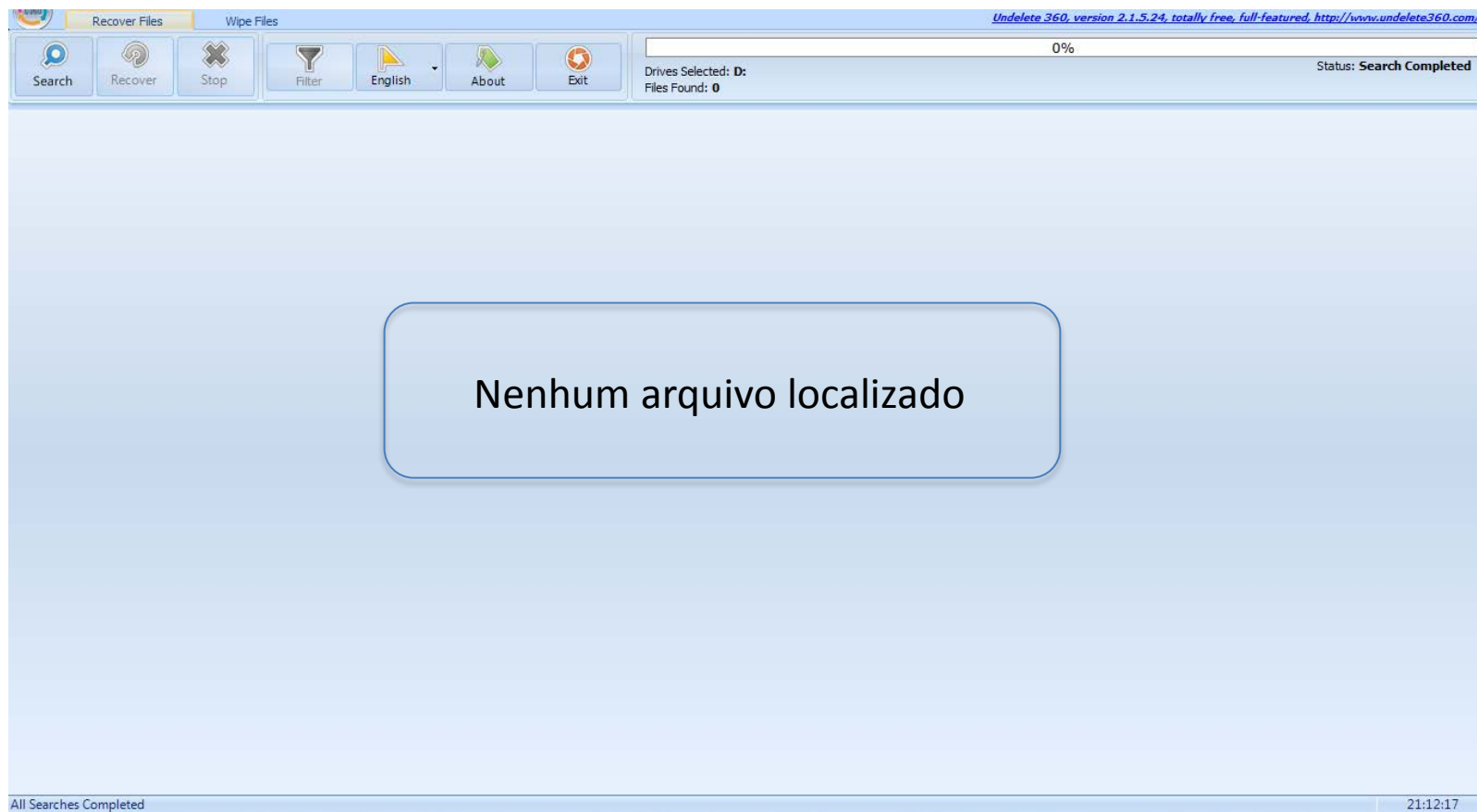
The screenshot displays a file wiping application window. At the top, a progress bar is at 100% with the status "Wipe Completed". The main area is titled "List of Folders and Files to be Wiped" and shows a dropdown menu for "US DoD 5220.22-M (3 passes)". Below this is a table with columns: Name, Type, Size, Modified, Attr, and Full Path. A modal dialog box is open in the center, titled "Wipe all previously deleted files". It contains the text "Wiping free space can take a substantial amount of time" and a "Close" button. The dialog has three checked options: "wipe directory entries", "wipe cluster tips", and "free disk space with MFT". A dropdown menu shows "PROTECTPEN (D:) - exFAT". Below the options, it says "Status: Wipe Completed" and shows a 100% progress bar. At the bottom left of the main window, it says "Wipe Completed".

Tempo médio para sanitização de um pendriver com capacidade de 7GB é de aproximadamente 1h30 min (dependendo da interface e processamento) USB 2.0 = 1h15

Método DOD 5220.22-M (3 passos)

Vulnerabilidades dos dispositivos móveis

Recuperação após a sanitização do Dispositivo móvel - Pendrive



Aplicação: Undelete 360

Método DOD 5220.22-M (3 passos)

Vulnerabilidades dos dispositivos móveis

Recuperação após a sanitização do Dispositivo móvel - Pendrive

Selecione os arquivos que você deseja recuperar marcando as caixas e depois apertando Recuperar.
Para melhores resultados recupere os arquivos em um dispositivo diferente.

Trocar para o modo avançado

<input type="checkbox"/>	Nome do arquivo	Caminho	Última modifica...	Tamanho	Estado	Comentário
<div style="border: 1px solid #ccc; border-radius: 15px; padding: 20px; display: inline-block;">Nenhum arquivo localizado</div>						

exFAT, 7,20 GB. Tamanho do cluster: 32768. Found 0 file(s) in 0.75 sec.

Recuperar...

Aplicação: Recuva

Método DOD 5220.22-M (3 passos)



FORENSE DIGITAL

Dados – Informação – Conhecimento – Sabedoria

Forense Digital – Pós Incidente

Mídias – Dados – Informações – Vestígios – Evidencias - Provas

1. Coleta

1. Isolar a area
2. Fotografar o cenário
3. Analisar o cenário
4. Coletar as evidencias
5. Garantir a integridade
6. Identificar as evidencias
7. Embalar as evidencias
8. Etiquetar as evidencias
9. Cadeia de custodia

2. Exame

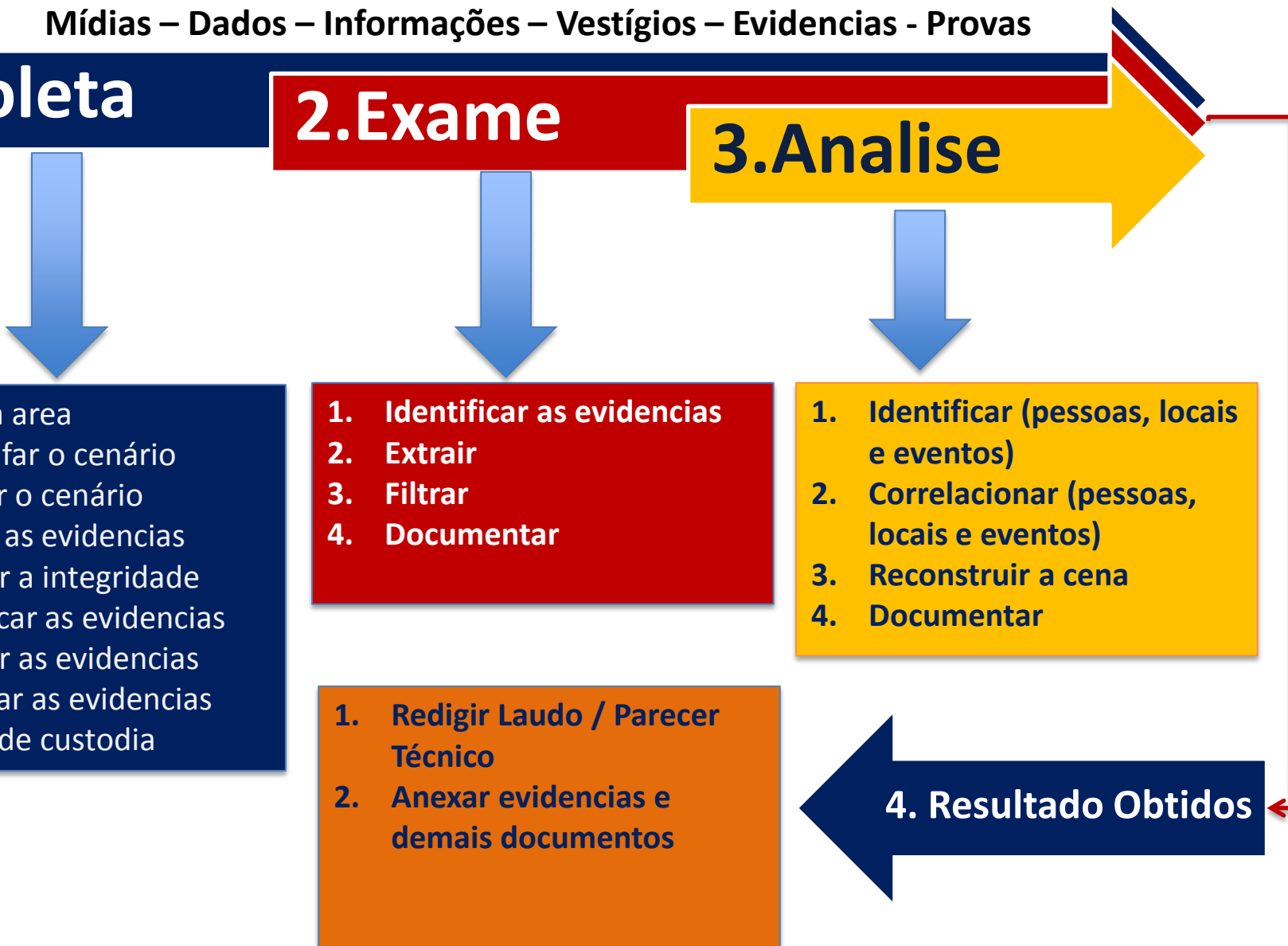
1. Identificar as evidencias
2. Extrair
3. Filtrar
4. Documentar

1. Redigir Laudo / Parecer Técnico
2. Anexar evidencias e demais documentos

3. Analise

1. Identificar (pessoas, locais e eventos)
2. Correlacionar (pessoas, locais e eventos)
3. Reconstruir a cena
4. Documentar

4. Resultado Obtidos



Forense Digital

Quando um crime é cometido, as evidências precisam ser coletadas da cena. Neste sentido uma equipe especializada salvaguardará o local e realizará todas as atividades necessárias na cena do crime para evitar a contaminação do cenário. Gravar as imagens e fotografar as cenas do crime, da vítima (caso haja), e todos os vestígios que constituam uma evidência / prova.



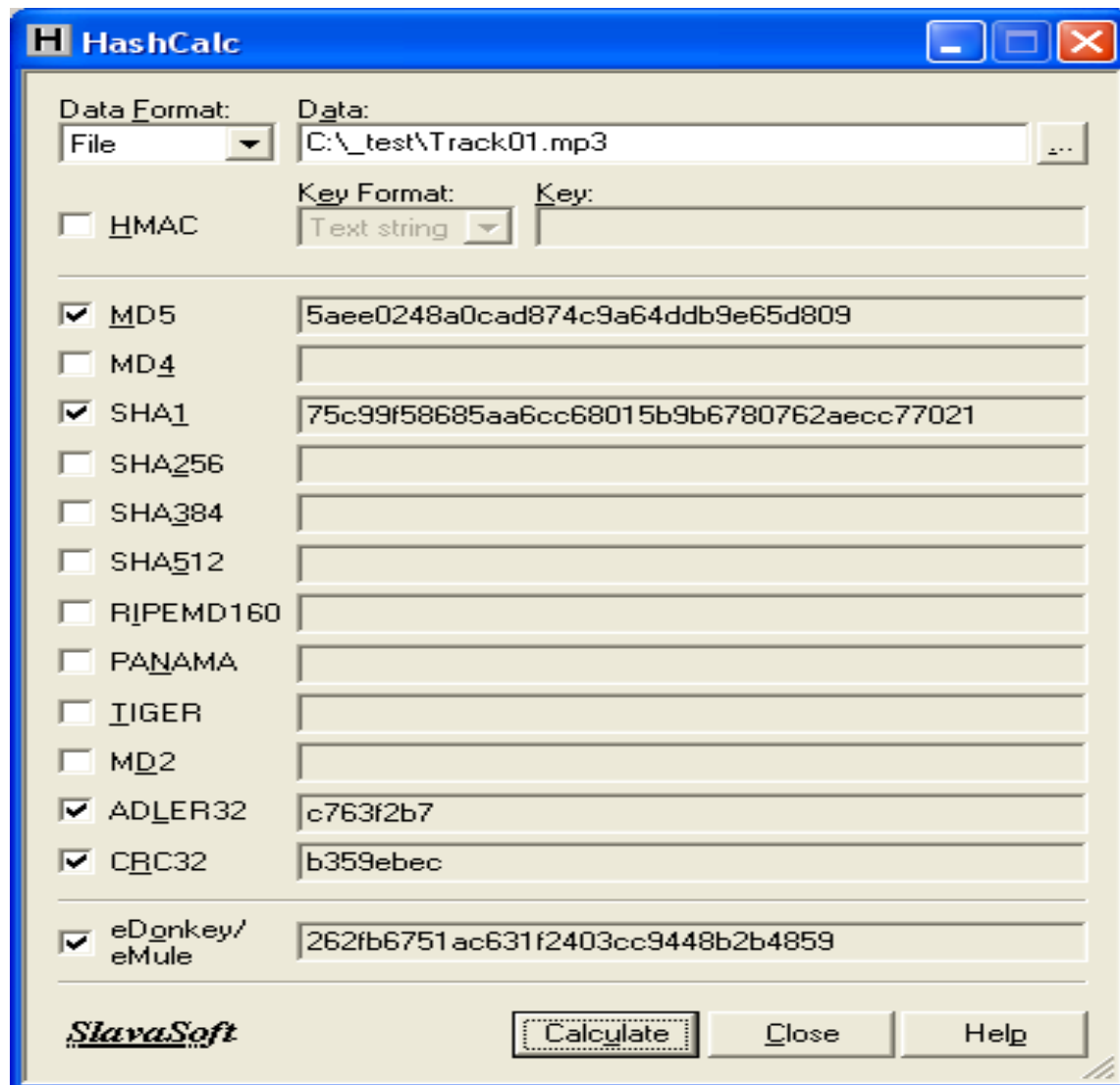
Sobre Forense Digital

A Computação Forense consiste, basicamente, no uso de **MÉTODOS CIENTÍFICOS** para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital. A aplicação desses métodos nem sempre se dá de maneira simples.

Forense Digital – Pós Incidente - HELIX



Hashe Assinatura Digital





Forense Digital – LOCARD

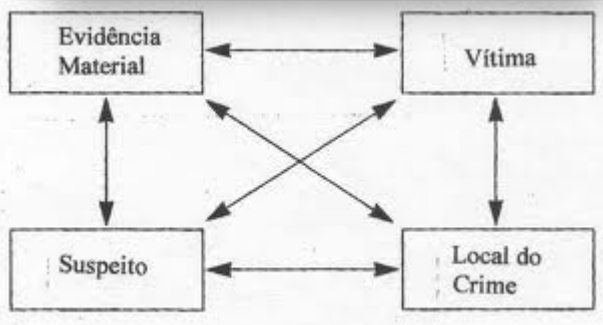
O princípio de Locard é aplicável nas cenas do crime, no qual o interveniente (ou intervenientes) da cena do crime entra em contacto com a própria cena onde o crime foi executado, trazendo algo para a cena do crime. *Cada contato deixa o seu rastro.*



Os fragmentos das provas são qualquer tipo de material deixado pelo criminoso (ou tiradas pelo mesmo) na cena do crime, ou o resultado do contato entre duas superfícies, exemplo impressão digital.

Os 2 Princípios da Criminalística:

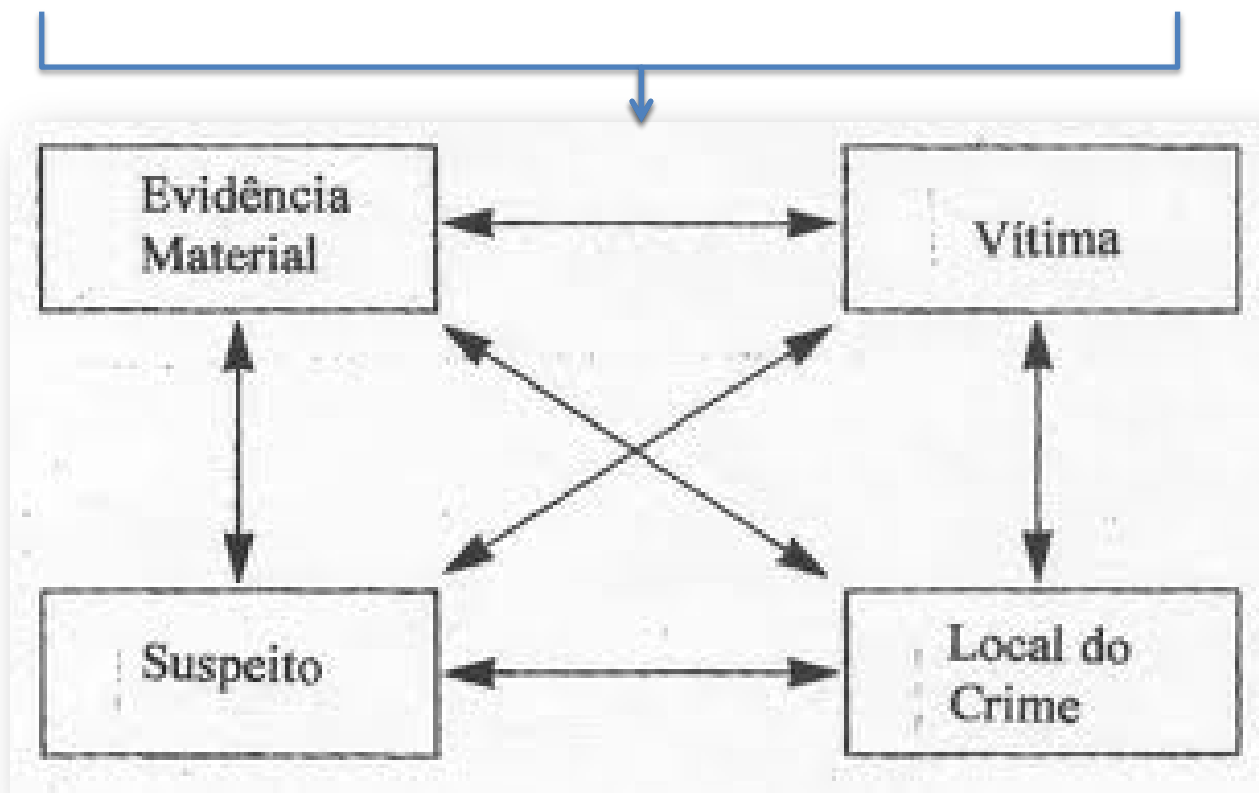
- **Princípio de Locard (1877-1966):** “Todo o contacto deixa um rastro (vestígio)”
- **Princípio da Individualidade:** “Dois objectos podem parecer indistinguíveis, mas não há dois objectos absolutamente idênticos”



Forense Digital – MATERIALIDADE X AUTORIA

Materialidade do fato

Autoria do fato



O perito deve atuar com total imparcialidade em seus laudos e pareceres.

Nota: Nunca prometa nada a um cliente sem antes analisar todos os fatos, vestígios e provas.

Forense Digital – CADEIA DE CUSTODIA

Há duas questões essenciais para a credibilidade da prova material:

A continuidade da prova que assegura-se através da preservação e registro da cena do crime e da não contaminação das amostras e vestígios recolhidos (assinalando os locais onde foram recolhidos)



Cadeia de custódia é assegurada através da embalagem, etiquetagem e armazenagem das amostras e vestígios (de modo a assinalar as circunstâncias e locais onde foram recolhidos) e seu transporte correto até ao laboratório e, uma vez analisados, eventualmente até ao Tribunal.

Nota: Não comprometa a evidencia em nenhuma hipótese. Atualmente é comum encontrar evidências etiquetadas diretamente no objeto de pericia pelo perito.

FORMULÁRIO DE CADEIA DE CUSTÓDIA						
NÚMERO DO CASO		20090226				
DETALHES DA MÍDIA OU EQUIPAMENTO						
ITEM	DESCRIÇÃO					
1	HD DO NOTEBOOK COM 2 GB DE CAPACIDADE					
FABRICANTE		MODELO		NÚMERO DE SÉRIE		
SAMSUNG		SGM2GB		ABC123456		
SOBRE A IMAGEM DOS DADOS						
DATA	HORA	CRIADA POR		FERRAMENTA USADA		
26/2/2009	10:53	SÍLVIO DO MONTE		EnCASE VERSION 3		
TIPO DE CÓPIA		HASH				
DISCO COMPLETO		4e3d2d5e5427953d7eda6ddc6627bf6b				
CADEIA DE CUSTÓDIA						
CÓDIGO	ORIGEM	DATA	HORA	DESTINO	DATA	HORA
1	LOCAL DE APREENSÃO	26/2/2009	17:00	PERÍCIA	26/2/2009	17:30

Forense Digital – DUPLICAÇÃO BIT-A-BIT



Forense Digital – DUPLICAÇÃO BIT-A-BIT

Recurso	Método	Tamanho do bloco	Tempo gasto HD 80 GB	Tempo gasto HD 160 GB
Encase	Sem compactação	2 GB	00:42:04	01:25:05
Encase	Compactação máxima	2 GB	00:43:40	01:21:01
Tableau Imager	Sem compactação	2 GB	00:33:20	01:04:29
Tableau Imager	Compactação máxima	2 GB	00:33:42	01:06:32
FTK Imager	Sem compactação	2 GB	00:53:29	01:44:55
FTK Imager	Compactação máxima	2 GB	00:55:46	01:50:44
SOLO 4	Sem compactação	2 GB	01:05:29	02:09:34
SOLO 4	Compactação máxima	2 GB	08:57:43	16:16:46

Forense Digital – DUPLICAÇÃO BIT-A-BIT



Forense Digital – DUPLICAÇÃO BIT-A-BIT










AUDITORIA - PREVENÇÃO FORENSE DIGITAL-

Dados – Informação – Conhecimento – Sabedoria

Escolha a conta que você deseja alterar

 root Administrador	 mPFin Usuário padrão
 mPSec Usuário padrão	 mPSICI Usuário padrão
 Convidado A conta de convidado está desativada	

[Criar uma nova conta](#)

[O que é uma conta de usuário?](#)

Operações adicionais que você pode executar

 [Configurar Controles dos Pais](#)

[Ir para a página Contas de Usuário principal](#)


















AREA DE TRABALHO TRADICIONAL – NÃO RECOMENDADA



Gerenciador de Tarefas do Windows

Arquivo Opções Exibir Janelas Ajuda

Aplicativos Processos Serviços Desempenho Rede Usuários

Tarefa	Status
 A receber - acesso@menospapel.com.br - Microsoft Outlook	Executando
 Apresentação 1 - Microsoft PowerPoint uso não comercial	Executando
 BluetoothView	Executando
 C:\windows\system32\cmd.exe	Executando
 C:\windows\system32\cmd.exe - ping www.google.com -t	Executando
 ENGENHARIA SOCIAL ErasmoGuimaraes_v8 - Microsoft PowerPoint ...	Executando
 Infi-Cyberinvestigacao-ErasmoGuimaraes-v8 - Microsoft PowerPoint ...	Executando
 Monitor the Bluetooth activity around you - Mozilla Firefox	Executando
 O Internet Explorer não pode exibir a página da Web - Windows Int...	Executando
 Sem título - Paint	Executando
 Skype™ - itversalabs	Executando
 Software Launcher	Executando
 Take This Lollipop - Google Chrome	Executando

VOCÊ ANALISA O SEU GERENCIADO DE TAREFAS?

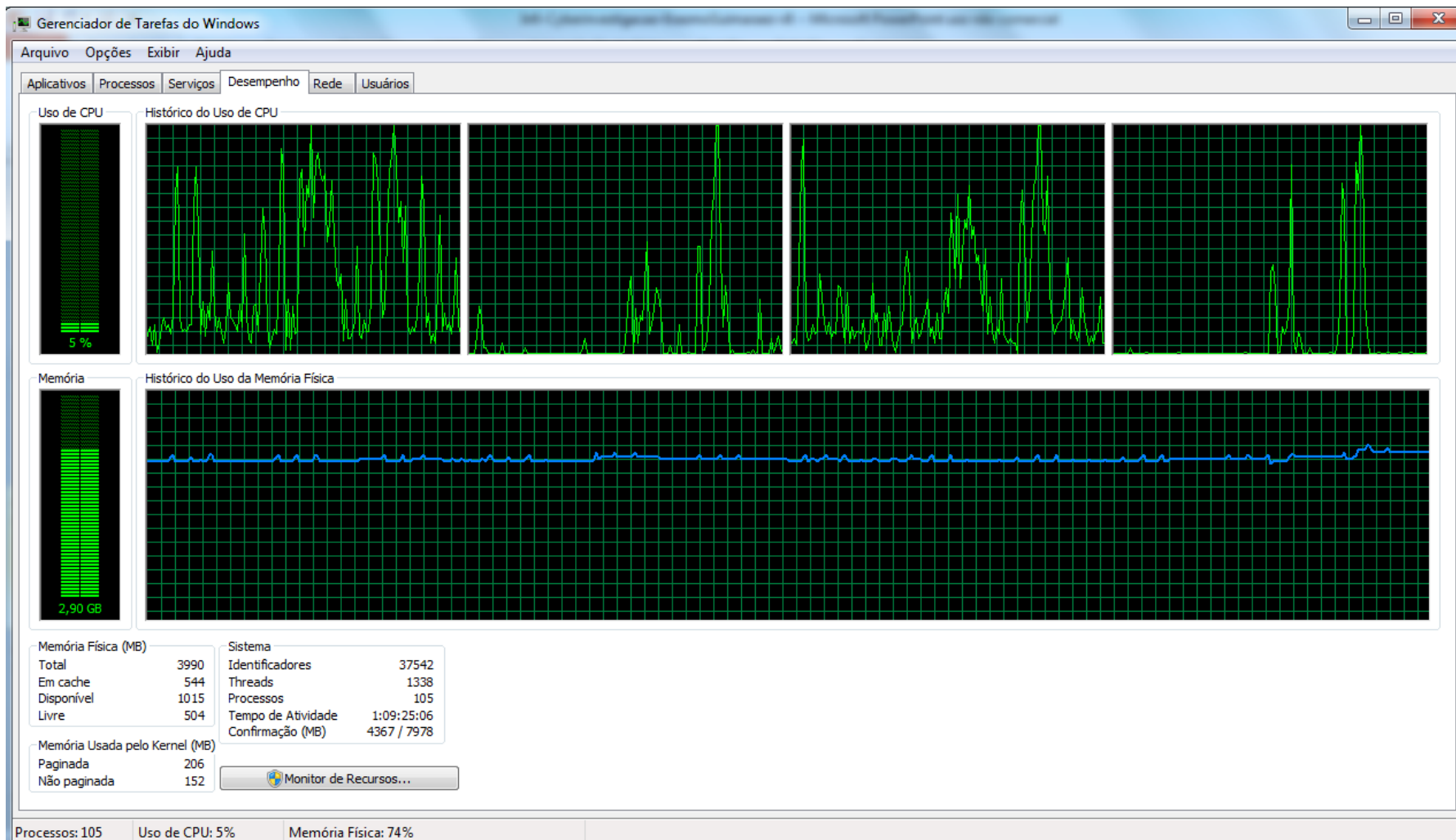
QUAIS PROCESSOS ESTÃO EM EXECUÇÃO?

Nome da Imagem	Nome de Usuário	CPU	Memória (Conjunto d...	Descrição
firefox.exe *32	mPSec	01	906.704 K	Firefox
POWERPNT.EXE	mPSec	00	148.648 K	Microsoft PowerPoint
Skype.exe *32	mPSec	01	80.560 K	Skype
chrome.exe *32	mPSec	00	73.844 K	Google Chrome
mspaint.exe	mPSec	00	61.288 K	Paint
chrome.exe *32	mPSec	01	47.516 K	Google Chrome
OUTLOOK.EXE	mPSec	01	45.064 K	Microsoft Outlook
chrome.exe *32	mPSec	00	40.780 K	Google Chrome
explorer.exe	mPSec	00	37.720 K	Windows Explorer
dwm.exe	mPSec	00	34.124 K	Gerenciador de Janelas da Área de Trabalho
chrome.exe *32	mPSec	00	23.348 K	Google Chrome
chrome.exe *32	mPSec	00	11.424 K	Google Chrome
Software Launcher.exe *32	mPSec	00	5.232 K	Software Launcher
iexplore.exe *32	mPSec	00	4.792 K	Internet Explorer
FlashPlayerPlugin_11_5_502_149.exe *32	mPSec	00	3.848 K	Adobe Flash Player 11.5 r502
taskmgr.exe	mPSec	01	2.864 K	Gerenciador de Tarefas do Windows
iexplore.exe *32	mPSec	00	2.440 K	Internet Explorer
csrss.exe	mPSec	00	1.724 K	
BluetoothView.exe *32	mPSec	00	1.720 K	BluetoothView
plugin-container.exe *32	mPSec	00	1.572 K	Plugin Container for Firefox
taskhost.exe	mPSec	00	1.400 K	Processo de Host para Tarefas do Windows
dmhcore.exe *32	mPSec	00	1.212 K	Easy Display Manager
rundll32.exe	mPSec	00	1.200 K	Processo de host do Windows (Rundll32)
iTunesHelper.exe *32	mPSec	00	1.180 K	iTunesHelper
BingBar.exe *32	mPSec	00	1.076 K	Extensões Cliente Bing
TrueCrypt.exe *32	mPSec	00	956 K	TrueCrypt
FlashPlayerPlugin_11_5_502_149.exe *32	mPSec	00	924 K	Adobe Flash Player 11.5 r502
jusched.exe *32	mPSec	00	872 K	Java(TM) Update Scheduler
MovieColorEnhancer.exe *32	mPSec	00	832 K	MovieColorEnhancer.exe
winlogon.exe	mPSec	00	800 K	
taskeng.exe	mPSec	00	748 K	Mecanismo do Agendador de Tarefas
PING.EXE	mPSec	00	728 K	Comando Ping do TCP/IP
Bi...	mPSec	00	698 K	Processo de Aplicativo Bing Cliente

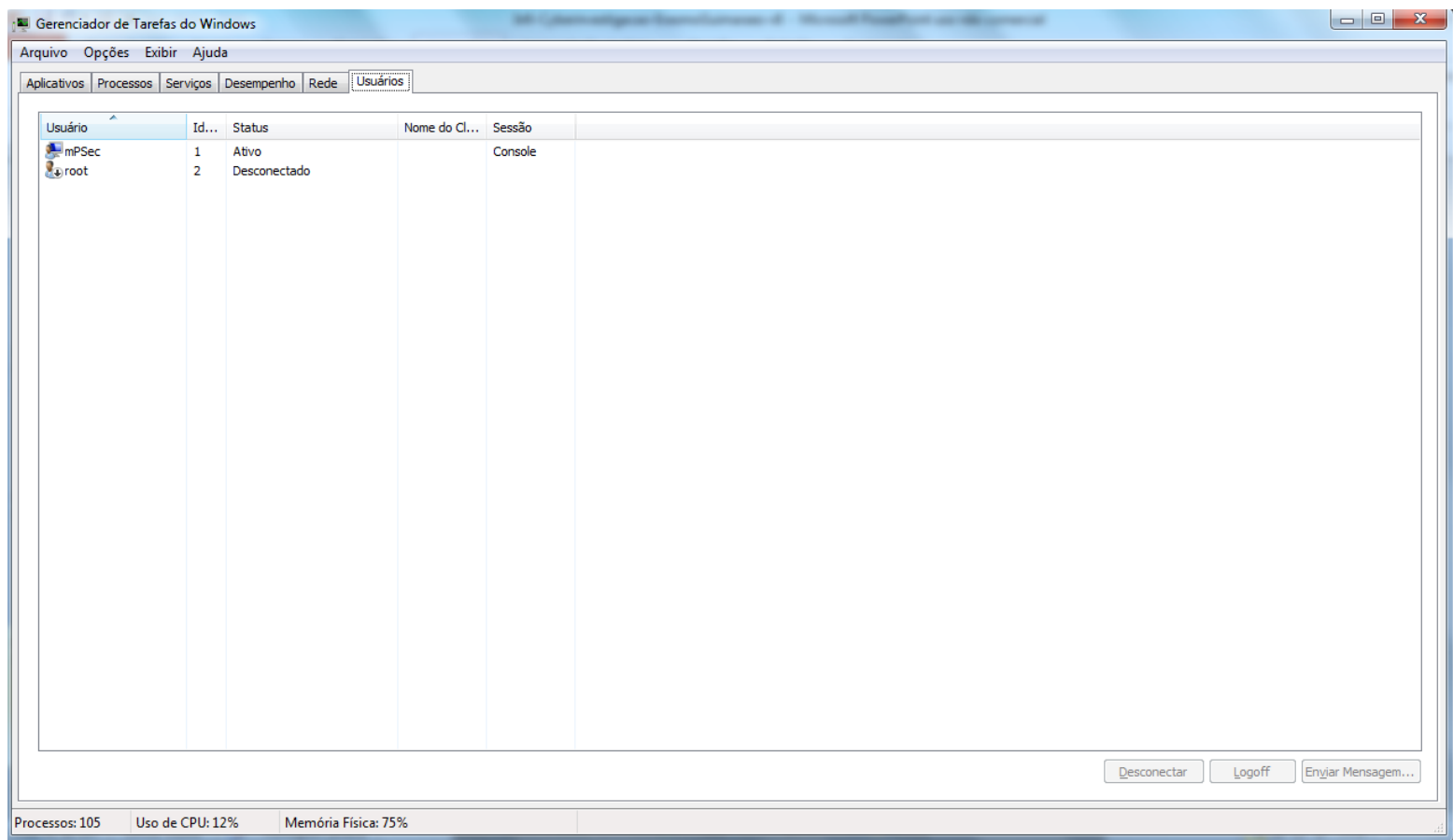
Mgstrar processos de todos os usuários

CSRSS.EXE
WINLOGON.EXE

CONSUMO DE CPU E MEMORIA



USUARIOS LOGADOS NO SISTEMA



USUARIOS LOGADOS NO SISTEMA

Monitor de Recursos

Arquivo Monitor Ajuda

Visão Geral CPU Memória Disco Rede

CPU 24% de Uso de CPU 84% de Frequência Máxima

Imagem	PID	Descrição	Status	Threads	CPU	CPU Média
System	4	NT Kernel & System	Em execução	167	0	0.36
firefox.exe	4428	Firefox	Em execução	53	17	5.25
svchost.exe (netsvcs)	1028	Processo de Host para Serviços do Windows	Em execução	43	0	0.00
OUTLOOK.EXE	3292	Microsoft Outlook	Em execução	38	0	0.03
Skype.exe	1216	Skype	Em execução	37	1	0.69
explorer.exe	3060	Windows Explorer	Em execução	34	0	0.17
chrome.exe	1136	Google Chrome	Em execução	33	0	0.00
taskmgr.exe	5564	Gerenciador de Tarefas do Windows	Em execução	32	0	0.30
svchost.exe (NetworkService)	1256	Processo de Host para Serviços do Windows	Em execução	24	0	0.00
explorer.exe	6336	Windows Explorer	Em execução	23	0	0.01
chrome.exe	5060	Google Chrome	Em execução	21	0	0.02
EvtEng.exe	1968	Intel(R) PROSet/Wireless Event Log Service	Em execução	21	0	0.00
svchost.exe (LocalSystemNet...)	872	Processo de Host para Serviços do Windows	Em execução	20	0	0.08
perfmom.exe	4164	Monitor de Recursos e Desempenho	Em execução	19	3	4.36
svchost.exe (LocalServiceNo...)	1568	Processo de Host para Serviços do Windows	Em execução	19	0	0.03
lsass.exe	764	Local Security Authority Process	Em execução	19	0	0.03
svchost.exe (LocalServiceNet...)	484	Processo de Host para Serviços do Windows	Em execução	18	0	0.00
csrss.exe	708	Processo do tempo de Execução do Servidor do Cliente	Em execução	17	0	0.16
POWERPNT.EXE	1208	Microsoft PowerPoint	Em execução	17	0	0.01
SearchIndexer.exe	3724	Indexador do Microsoft Windows Search	Em execução	16	0	0.00
wlanext.exe	1412	Windows Wireless LAN 802.11 Extensibility Framework	Em execução	14	0	0.00
svchost.exe (LocalServiceAn...)	3136	Processo de Host para Serviços do Windows	Em execução	14	0	0.00
UNS.exe	2064	User Notification Service	Em execução	14	0	0.00
spoolsv.exe	1524	Aplicativo de subsistema de spooler	Em execução	13	0	0.00

Disco 4 KB/s de E/S de Disco 0% Mais Longo Tempo em Atividade

Rede 0 Kbps de E/S de Rede 0% de Utilização da Rede

Memória 0 Falhas Graves/s 75% de Memória Física Usada

Exibições

CPU 100%

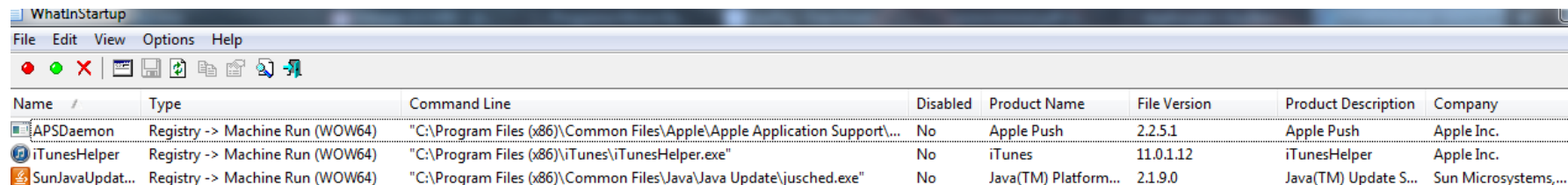
60 Segundos

Disco 100 KB/s

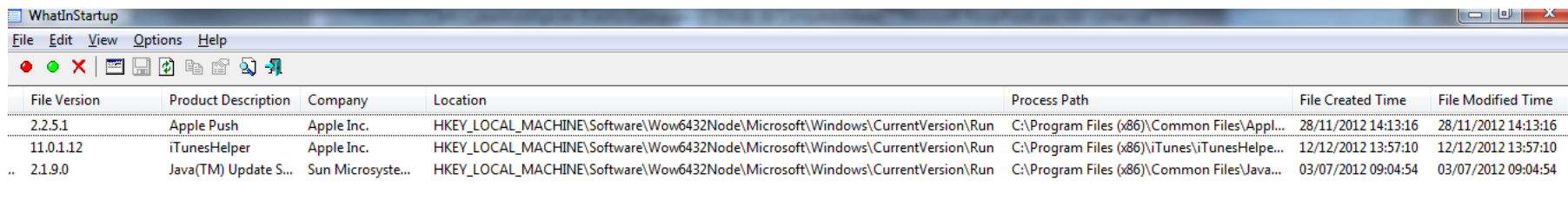
Rede 10 Kbps

Memória 100 Falhas Graves/s

Inicialização automática de programas instalados



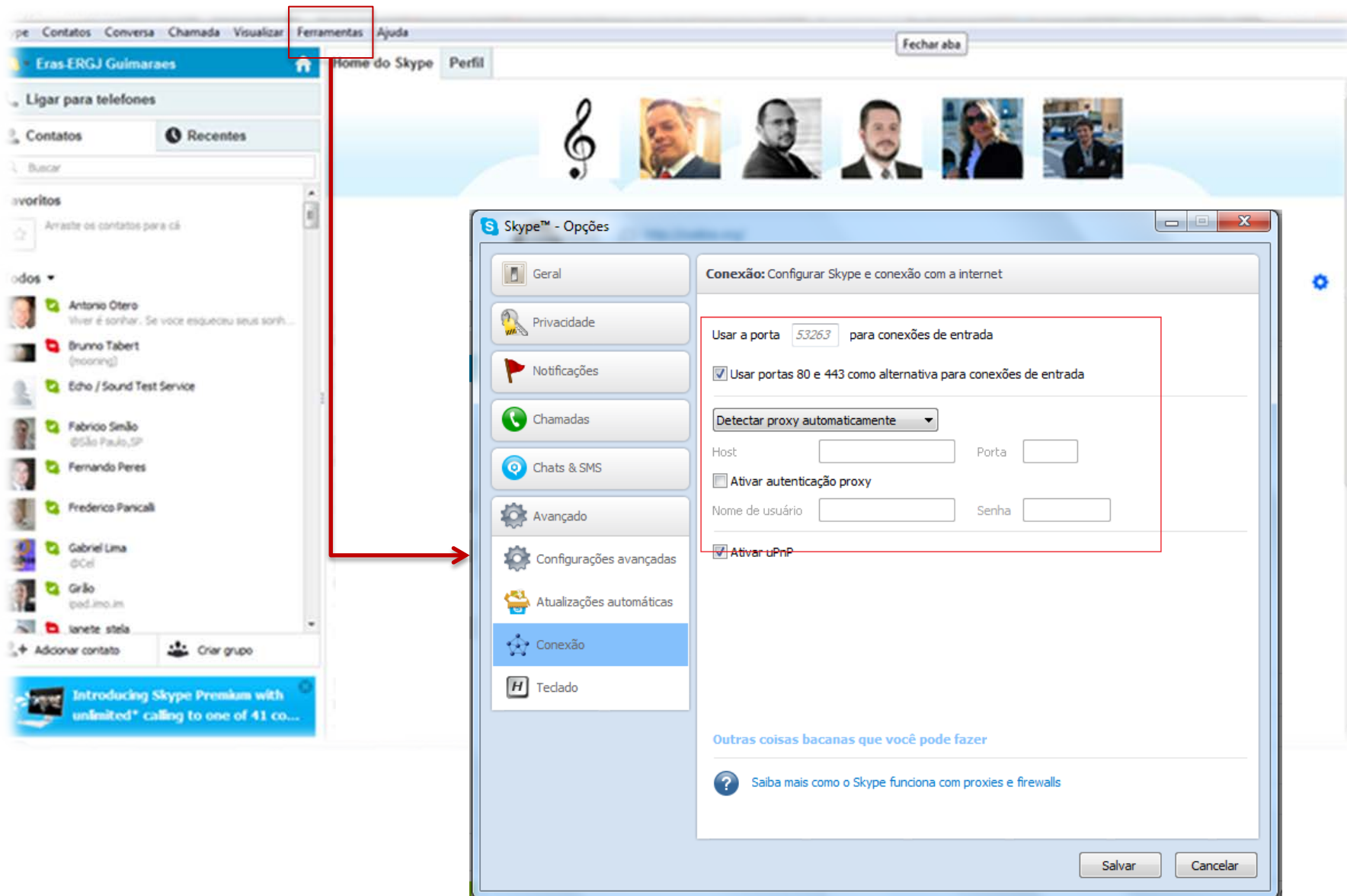
Name	Type	Command Line	Disabled	Product Name	File Version	Product Description	Company
APSDaemon	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\Common Files\Apple\Apple Application Support\...	No	Apple Push	2.2.5.1	Apple Push	Apple Inc.
iTunesHelper	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\iTunes\iTunesHelper.exe"	No	iTunes	11.0.1.12	iTunesHelper	Apple Inc.
SunJavaUpdat...	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"	No	Java(TM) Platform...	2.1.9.0	Java(TM) Update S...	Sun Microsystems,...



File Version	Product Description	Company	Location	Process Path	File Created Time	File Modified Time
2.2.5.1	Apple Push	Apple Inc.	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	C:\Program Files (x86)\Common Files\Appl...	28/11/2012 14:13:16	28/11/2012 14:13:16
11.0.1.12	iTunesHelper	Apple Inc.	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	C:\Program Files (x86)\iTunes\iTunesHelve...	12/12/2012 13:57:10	12/12/2012 13:57:10
.. 2.1.9.0	Java(TM) Update S...	Sun Microsyste...	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	C:\Program Files (x86)\Common Files\Java...	03/07/2012 09:04:54	03/07/2012 09:04:54

Fique atento aos programas configurados arbitrariamente

CACHES – SKYPE



The image shows the Skype desktop application interface. The top menu bar includes 'Arquivo', 'Contatos', 'Conversa', 'Chamada', 'Visualizar', 'Ferramentas', and 'Ajuda'. The 'Ferramentas' menu is highlighted with a red box, and a red arrow points from it to the 'Opções' dialog box. The 'Opções' dialog box is open to the 'Conexão' (Connection) tab. A red box highlights the 'Conexão' settings area, which includes:

- Usar a porta para conexões de entrada
- Usar portas 80 e 443 como alternativa para conexões de entrada
- Detector proxy automaticamente (dropdown menu)
- Host Porta
- Ativar autenticação proxy
- Nome de usuário Senha
- Ativar uPnP

At the bottom of the dialog box, there are 'Salvar' and 'Cancelar' buttons. A link at the bottom says 'Saiba mais como o Skype funciona com proxies e firewalls'.

CACHES – SKYPE

Skype™ - Opções

Configurações de privacidade: evite chamadas e chats que não quiser receber

Permitir chamadas de...

- qualquer pessoa
- somente pessoas entre os meus Contatos

Receber vídeo automaticamente e compartilhar tela com...

- qualquer um
- apenas pessoas na minha lista de contatos
- ninguém

Exibir que tenho webcam para...

- pessoas na minha lista de contatos
- ninguém

Permitir chats de...

- qualquer pessoa
- somente pessoas entre os meus Contatos

Manter histórico por

- continuuamente
- sem histórico
- 2 semanas
- 1 mês
- 3 meses
- continuamente

Permitir a exibição do meu status na web

Aceitar os cookies Skype do Browser Apre...

Permitir anúncios direcionados da Microsoft, inclusive o uso da idade e sexo contidos no perfil Skype. [Saiba mais](#)

Skype Chat






Record Number	Action Type	Action Time	User Name	Display Name	Duration	Chat Message	ChatID
13384	Chat Message	01/12/2011 16:47:16	adr_lu	Ac		tava	# bs/\$ac li...
13387	Chat Message	01/12/2011 16:48:22	adr_lu	Ac		eh n	# tao # bs/\$ac li...
13388	Chat Message	01/12/2011 16:48:38	adr_lu	Ac		é q z	# # bs/\$ac li...
13391	Chat Message	01/12/2011 16:51:06	adr_lu	Ac		é ac	# # bs/\$ac li...
13395	Chat Message	01/12/2011 16:51:43	adr_lu	Ac		sim	# # bs/\$ac li...
13396	Chat Message	01/12/2011 16:51:44	adr_lu	Ac		fo	# # bs/\$ac li...
13397	Chat Message	01/12/2011 16:51:47	adr_lu	Ac		mul	# # bs/\$ac li...
13398	Chat Message	01/12/2011 16:52:04	adr_lu	Ac		era r	# # bs/\$ac li...
13399	Chat Message	01/12/2011 16:52:09	adr_lu	Ac		ja q	# # bs/\$ac li...
13400	Chat Message	01/12/2011 16:52:21	adr_lu	Ac		pior	# por isso # bs/\$ac li...
13403	Chat Message	01/12/2011 16:56:06	adr_lu	Ac		po r	# um em... # bs/\$ac li...
13404	Chat Message	01/12/2011 16:56:12	adr_lu	Ac		é fal	# # bs/\$ac li...
13406	Chat Message	01/12/2011 16:56:47	adr_lu	Ac		leml	# # bs/\$ac li...
13409	Chat Message	01/12/2011 16:57:15	adr_lu	Ac		vc	# # bs/\$ac li...
13411	Chat Message	01/12/2011 16:57:28	adr_lu	Ac		boa	# # bs/\$ac li...

Skype Ligações realizada



Record Number	Action Type	Action Time	User Name	Display Name	Duration
14117	Outgoing Call	04/12/2011 12:07:48	+55116899	+55116899	00:00:15
14211	Outgoing Call	05/12/2011 11:52:10	+55116899	+55116899	00:16:51
11581	Outgoing Call	25/11/2011 13:41:09	+55116687	+55116687	00:01:30
14072	Outgoing Call	03/12/2011 20:50:11	+55115212	+55115212	
14078	Outgoing Call	03/12/2011 20:50:29	+55115212	+55115212	
14083	Outgoing Call	03/12/2011 20:50:42	+55115212	+55115212	
14088	Outgoing Call	03/12/2011 21:01:40	+55115212	+55115212	
2089	Outgoing Call	14/10/2011 17:18:23	+55115049	+55115049	00:01:51
11677	Outgoing Call	25/11/2011 14:05:06	+55114193	+55114193	00:00:10
11683	Outgoing Call	25/11/2011 14:05:38	+55114193	+55114193	00:03:53

C. ALTO COMPLETAR – RISCOS E EVIDENCIAS

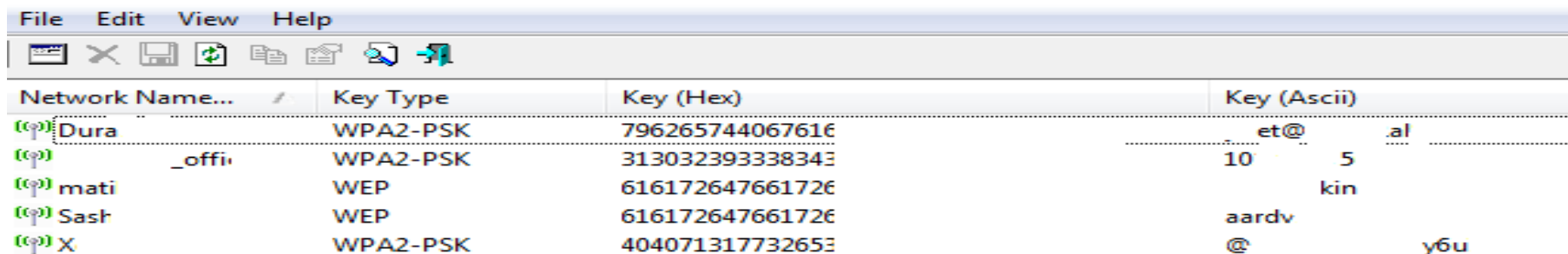
Senhas do Navegador em cache – Alto completar

URL	Web Browser	User Name	Password
 http://hotel.habbinfo.com.br	Firefox 3.5/4	el	1234!
 http://hotel.habbinfo.com.br	Firefox 3.5/4	el11	1234!
 http://hotel.habbinfo.com.br...	Chrome	el 11	1234!
 https://accounts.google.com	Firefox 3.5/4	_abriel @y...	1234!
 https://accounts.google.com/servicelogin	Internet Explorer 7.0 - 8.0	:om	

Senhas PST (outlook)

Filename	Encryption	Version	CRC Value	Password 1	Password 2	Password 3	Full Path	Size	Modified Date
 @gmail.com...	Compressible	23	0x00000000				C:\Users\ [User] \AppData\Local\Microsoft\Outlook	271.360	21/10/2011 23:05:18
 @gmail.com...	Compressible	23	0x00000000				C:\Users\ [User] \AppData\Local\Microsoft\Outlook	271.360	21/10/2011 22:56:23

Senhas Wi-Fi Digitadas no equipamento



Network Name...	Key Type	Key (Hex)	Key (Ascii)
(?) Dura	WPA2-PSK	796265744067616	et@ .al
(?) _offi	WPA2-PSK	313032393338343	10 5
(?) mati	WEP	616172647661726	kin
(?) Sash	WEP	616172647661726	aardv
(?) X	WPA2-PSK	404071317732653	@ y6u

Dispositivos Bluetooth

Device Name	Description	Address	Major Device T...	Minor Device ...	First Detected On	Last Detected On	Detection Cou...	No Detection ...	% Detection	Connected	Remember...	Authentica..
		f8:7b:7a:45:2a:df	Phone	Cellular	26/02/2013 13:15:32	26/02/2013 13:15:32	1	116	0.9%	No	No	No
		5c:17:d3:7c:62:0b	Phone	Cellular	26/02/2013 13:18:48	26/02/2013 13:18:48	1	109	0.9%	No	No	No
		b8:f9:34:ea:98:3d	Phone	Cellular	26/02/2013 13:24:34	26/02/2013 13:24:34	1	96	1.0%	No	No	No
		00:26:ff:5c:2d:5b	Phone	Smart	26/02/2013 13:39:54	26/02/2013 13:39:54	1	66	1.5%	No	No	No
		00:0d:92:8b:c0:91	Phone	Cellular	26/02/2013 14:00:14	26/02/2013 14:00:14	1	26	3.7%	No	No	No
		c8:aa:21:08:0a:12	Phone	Cellular	26/02/2013 14:08:59	26/02/2013 14:08:59	1	9	10.0%	No	No	No
marina s.		00:25:e5:94:8f:02	Phone	Cellular	26/02/2013 13:19:10	26/02/2013 13:19:10	1	108	0.9%	No	No	No
Cynthia	Cynthia	74:a7:22:77:c6:0e	Phone	Cellular	26/02/2013 14:21:51	26/02/2013 14:23:36	7	0	100.0%	No	No	No
E2262	E2262	14:f4:2a:a0:81:6d	Phone	Cellular	26/02/2013 13:19:58	26/02/2013 13:20:20	2	105	1.9%	No	No	No
Gee		98:4b:4a:5a:a5:c6	Phone	Cellular	26/02/2013 13:23:14	26/02/2013 13:23:14	1	99	1.0%	No	No	No
Grell e sebby	Grell e sebby	6f:2b:bb:1d:66:12	Phone	Cellular	26/02/2013 14:21:51	26/02/2013 14:23:17	3	4	42.9%	No	No	No
GT-E2550L		bc:47:60:5f:4d:a5	Phone	Cellular	26/02/2013 13:20:20	26/02/2013 13:20:20	1	105	0.9%	No	No	No
LG-C300		74:a7:22:72:7f:b0	Phone	Cellular	26/02/2013 13:19:58	26/02/2013 13:19:58	1	106	0.9%	No	No	No
LG-C365		a8:92:2c:89:50:6e	Phone	Cellular	26/02/2013 13:27:02	26/02/2013 13:27:02	1	91	1.1%	No	No	No
Nokia 110		38:19:2f:f1:ed:8f	Phone	Cellular	26/02/2013 13:52:05	26/02/2013 13:52:05	1	42	2.3%	No	No	No
Nokia N8-00		78:2e:ef:bd:2c:f7	Phone	Smart	26/02/2013 13:43:25	26/02/2013 13:43:25	1	59	1.7%	No	No	No
Nokia N81 8GB	Nokia N81 8GB	00:21:08:9c:24:9c	Phone	Smart	26/02/2013 14:21:51	26/02/2013 14:23:36	7	0	100.0%	No	No	No
Robertinho		98:4b:4a:2e:74:6f	Phone	Cellular	26/02/2013 13:16:57	26/02/2013 13:16:57	1	113	0.9%	No	No	No
£££		00:25:67:3c:b9:db	Phone	Cellular	26/02/2013 13:23:14	26/02/2013 13:23:14	1	99	1.0%	No	No	No

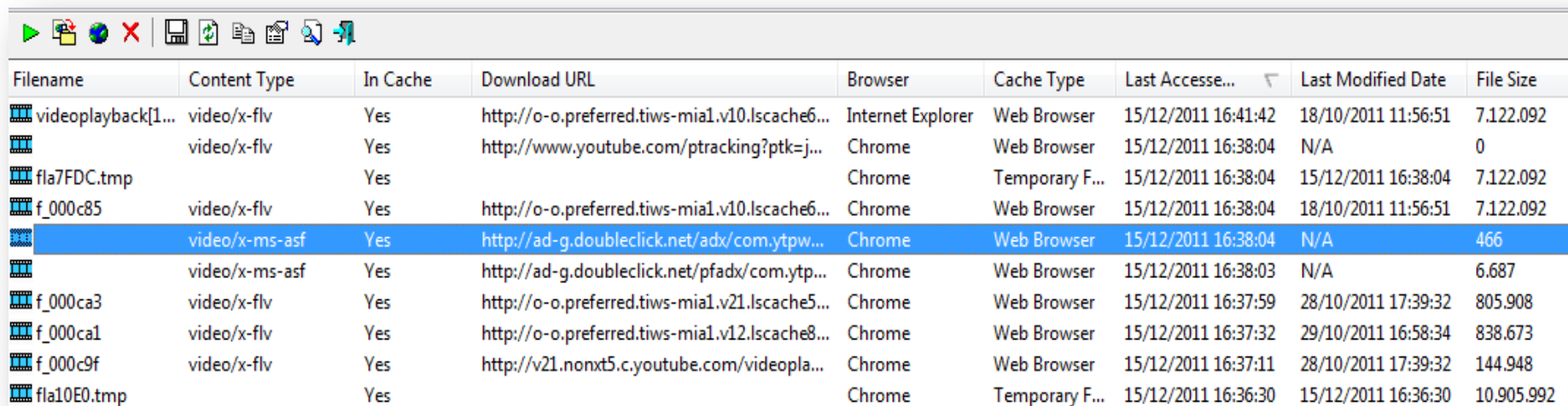
19 Bluetooth Devices, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

Ultimas Buscas na Web – Caso Email Fake

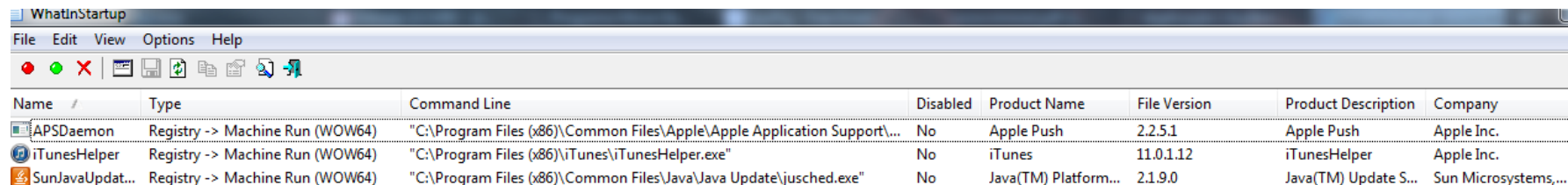
● rece	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● 03428729000149	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● CCBA CONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● ccba construcoes ltda epp	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● CCBCONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● CCBACONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● CCONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● CCONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● série/número 003/000001335	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
● 42210889@n07	Google	General	15/12/2011 01:43:07	Mozilla	1	http://www.google.com.br/...
● 42210889@N07	Google	General	15/12/2011 01:40:49	Mozilla	1	http://www.google.com.br/...
● streetviewer	Google	General	15/12/2011 01:23:37	Mozilla	1	http://www.google.com.br/...
● MY	Google	General	14/12/2011 23:42:28	Chrome	0	http://www.google.com.br/...

Últimos vídeos acessados

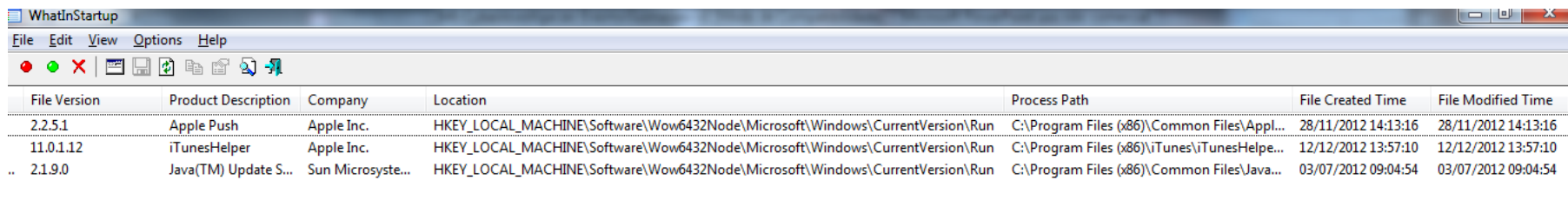


Filename	Content Type	In Cache	Download URL	Browser	Cache Type	Last Access...	Last Modified Date	File Size
videoplayback[1...	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v10.lscache6...	Internet Explorer	Web Browser	15/12/2011 16:41:42	18/10/2011 11:56:51	7.122.092
	video/x-flv	Yes	http://www.youtube.com/ptracking?ptk=j...	Chrome	Web Browser	15/12/2011 16:38:04	N/A	0
fla7FDC.tmp		Yes		Chrome	Temporary F...	15/12/2011 16:38:04	15/12/2011 16:38:04	7.122.092
f_000c85	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v10.lscache6...	Chrome	Web Browser	15/12/2011 16:38:04	18/10/2011 11:56:51	7.122.092
	video/x-ms-asf	Yes	http://ad-g.doubleclick.net/adx/com.ytpw...	Chrome	Web Browser	15/12/2011 16:38:04	N/A	466
	video/x-ms-asf	Yes	http://ad-g.doubleclick.net/pfadx/com.ytp...	Chrome	Web Browser	15/12/2011 16:38:03	N/A	6.687
f_000ca3	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v21.lscache5...	Chrome	Web Browser	15/12/2011 16:37:59	28/10/2011 17:39:32	805.908
f_000ca1	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v12.lscache8...	Chrome	Web Browser	15/12/2011 16:37:32	29/10/2011 16:58:34	838.673
f_000c9f	video/x-flv	Yes	http://v21.nonxt5.c.youtube.com/videopla...	Chrome	Web Browser	15/12/2011 16:37:11	28/10/2011 17:39:32	144.948
fla10E0.tmp		Yes		Chrome	Temporary F...	15/12/2011 16:36:30	15/12/2011 16:36:30	10.905.992

Inicialização automática de programas instalados



Name	Type	Command Line	Disabled	Product Name	File Version	Product Description	Company
APSDaemon	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\Common Files\Apple\Apple Application Support\...	No	Apple Push	2.2.5.1	Apple Push	Apple Inc.
iTunesHelper	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\iTunes\iTunesHelper.exe"	No	iTunes	11.0.1.12	iTunesHelper	Apple Inc.
SunJavaUpdat...	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"	No	Java(TM) Platform...	2.1.9.0	Java(TM) Update S...	Sun Microsystems,...

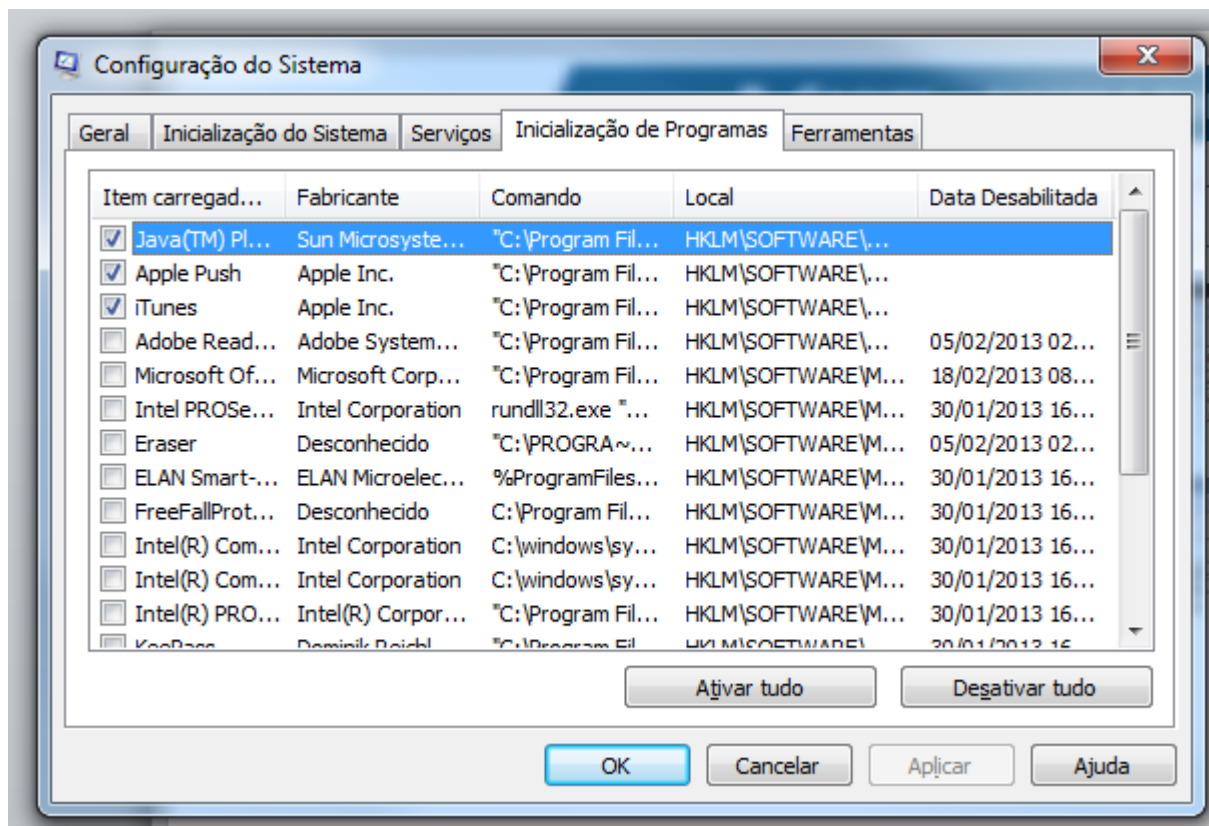


File Version	Product Description	Company	Location	Process Path	File Created Time	File Modified Time
2.2.5.1	Apple Push	Apple Inc.	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	C:\Program Files (x86)\Common Files\Appl...	28/11/2012 14:13:16	28/11/2012 14:13:16
11.0.1.12	iTunesHelper	Apple Inc.	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	C:\Program Files (x86)\iTunes\iTunesHelve...	12/12/2012 13:57:10	12/12/2012 13:57:10
.. 2.1.9.0	Java(TM) Update S...	Sun Microsyste...	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	C:\Program Files (x86)\Common Files\Java...	03/07/2012 09:04:54	03/07/2012 09:04:54

Fique atento aos programas configurados arbitrariamente

Vulnerabilidades de sistemas - MSCONFIG






Inicialização automática de programas instalados





Fique atento aos programas que estão configurados para inicialização automática.

C. ALTO COMPLETAR – RISCOS E EVIDENCIAS

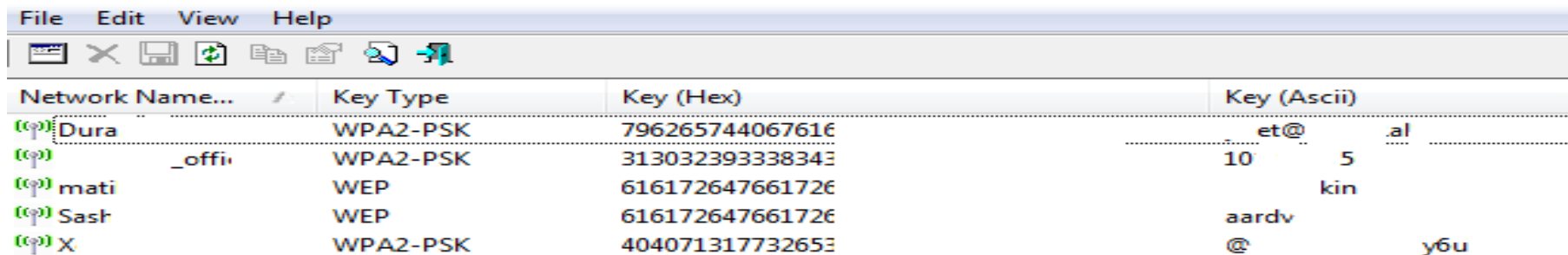
Senhas do Navegador em cache – Alto completar

URL	Web Browser	User Name	Password
 http://hotel.habbinfo. .com.br	Firefox 3.5/4	el	1234!
 http://hotel.habbinfo. .com.br	Firefox 3.5/4	el11	1234!
 http://hotel.habbinfo. .com.br...	Chrome	el 11	1234!
 https://accounts.google.com	Firefox 3.5/4	_abriel @y...	1234!
 https://accounts.google.com/servicelogin	Internet Explorer 7.0 - 8.0	:om	

Senhas PST (outlook)

Filename	Encryption	Version	CRC Value	Password 1	Password 2	Password 3	Full Path	Size	Modified Date
 @gmail.com...	Compressible	23	0x00000000				C:\Users\ [redacted] \AppData\Local\Microsoft\Outlook	271.360	21/10/2011 23:05:18
 @gmail.com...	Compressible	23	0x00000000				C:\Users\ [redacted] \AppData\Local\Microsoft\Outlook	271.360	21/10/2011 22:56:23

Senhas Wi-Fi Digitadas no equipamento



Network Name...	Key Type	Key (Hex)	Key (Ascii)
(e) Dura	WPA2-PSK	796265744067616	et@.al
(e) _offi	WPA2-PSK	313032393338343	10 5
(e) mati	WEP	616172647661726	kin
(e) Sash	WEP	616172647661726	aardv
(e) X	WPA2-PSK	404071317732653	@ y6u

C. BLUETOOTH – RISCOS E EVIDENCIAS

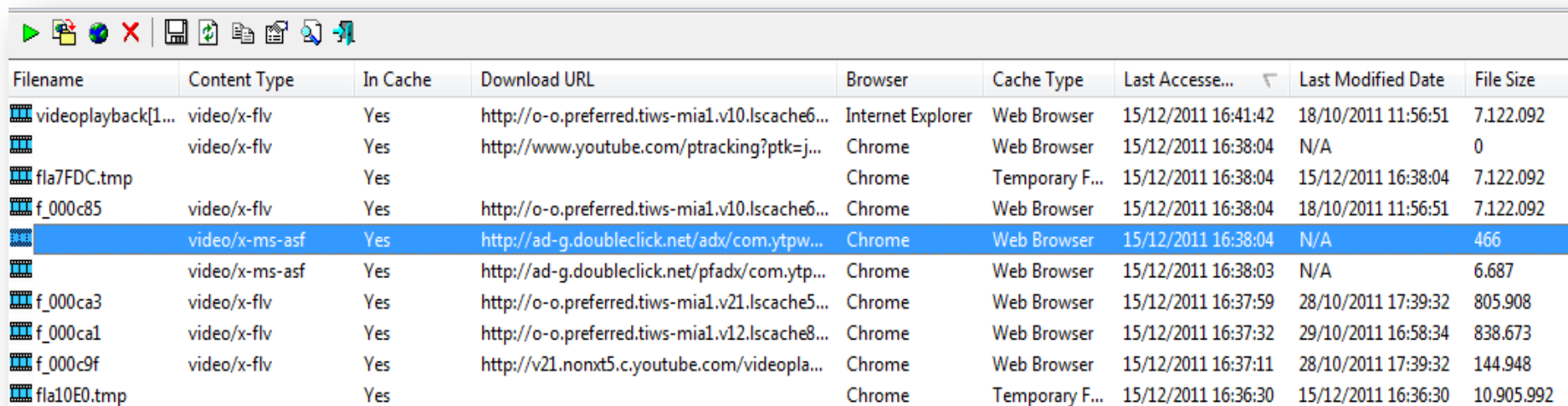
Dispositivos Bluetooth

Device Name	Description	Address	Major Device T...	Minor Device ...	First Detected On	Last Detected On	Detection Cou...	No Detection ...	% Detection	Connected	Remember...	Authentica..
		f8:7b:7a:45:2a:df	Phone	Cellular	26/02/2013 13:15:32	26/02/2013 13:15:32	1	116	0.9%	No	No	No
		5c:17:d3:7c:62:0b	Phone	Cellular	26/02/2013 13:18:48	26/02/2013 13:18:48	1	109	0.9%	No	No	No
		b8:f9:34:ea:98:3d	Phone	Cellular	26/02/2013 13:24:34	26/02/2013 13:24:34	1	96	1.0%	No	No	No
		00:26:ff:5c:2d:5b	Phone	Smart	26/02/2013 13:39:54	26/02/2013 13:39:54	1	66	1.5%	No	No	No
		00:0d:92:8b:c0:91	Phone	Cellular	26/02/2013 14:00:14	26/02/2013 14:00:14	1	26	3.7%	No	No	No
		c8:aa:21:08:0a:12	Phone	Cellular	26/02/2013 14:08:59	26/02/2013 14:08:59	1	9	10.0%	No	No	No
marina s.		00:25:e5:94:8f:02	Phone	Cellular	26/02/2013 13:19:10	26/02/2013 13:19:10	1	108	0.9%	No	No	No
Cynthia	Cynthia	74:a7:22:77:c6:0e	Phone	Cellular	26/02/2013 14:21:51	26/02/2013 14:23:36	7	0	100.0%	No	No	No
E2262	E2262	14:f4:2a:a0:81:6d	Phone	Cellular	26/02/2013 13:19:58	26/02/2013 13:20:20	2	105	1.9%	No	No	No
Gee		98:4b:4a:5a:a5:c6	Phone	Cellular	26/02/2013 13:23:14	26/02/2013 13:23:14	1	99	1.0%	No	No	No
Grell e sebby	Grell e sebby	6f:2b:bb:1d:66:12	Phone	Cellular	26/02/2013 14:21:51	26/02/2013 14:23:17	3	4	42.9%	No	No	No
GT-E2550L		bc:47:60:5f:4d:a5	Phone	Cellular	26/02/2013 13:20:20	26/02/2013 13:20:20	1	105	0.9%	No	No	No
LG-C300		74:a7:22:72:7f:b0	Phone	Cellular	26/02/2013 13:19:58	26/02/2013 13:19:58	1	106	0.9%	No	No	No
LG-C365		a8:92:2c:89:50:6e	Phone	Cellular	26/02/2013 13:27:02	26/02/2013 13:27:02	1	91	1.1%	No	No	No
Nokia 110		38:19:2f:f1:ed:8f	Phone	Cellular	26/02/2013 13:52:05	26/02/2013 13:52:05	1	42	2.3%	No	No	No
Nokia N8-00		78:2e:ef:bd:2c:f7	Phone	Smart	26/02/2013 13:43:25	26/02/2013 13:43:25	1	59	1.7%	No	No	No
Nokia N81 8GB	Nokia N81 8GB	00:21:08:9c:24:9c	Phone	Smart	26/02/2013 14:21:51	26/02/2013 14:23:36	7	0	100.0%	No	No	No
Robertinho		98:4b:4a:2e:74:6f	Phone	Cellular	26/02/2013 13:16:57	26/02/2013 13:16:57	1	113	0.9%	No	No	No
£££		00:25:67:3c:b9:db	Phone	Cellular	26/02/2013 13:23:14	26/02/2013 13:23:14	1	99	1.0%	No	No	No

Ultimas Buscas na Web – Caso Email Fake

rece	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
03428729000149	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
CCBA CONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
ccba construcoes ltda epp	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
CCBCONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
CCBACONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
CCCONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
CCONSTRUCOES LTDA EPP	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
série/número 003/000001335	Google	General	15/12/2011 03:00:11	Chrome	0	http://www.google.com.br/...
42210889@n07	Google	General	15/12/2011 01:43:07	Mozilla	1	http://www.google.com.br/...
42210889@N07	Google	General	15/12/2011 01:40:49	Mozilla	1	http://www.google.com.br/...
streetviewer	Google	General	15/12/2011 01:23:37	Mozilla	1	http://www.google.com.br/...
MY	Google	General	14/12/2011 23:42:28	Chrome	0	http://www.google.com.br/...

Últimos vídeos acessados

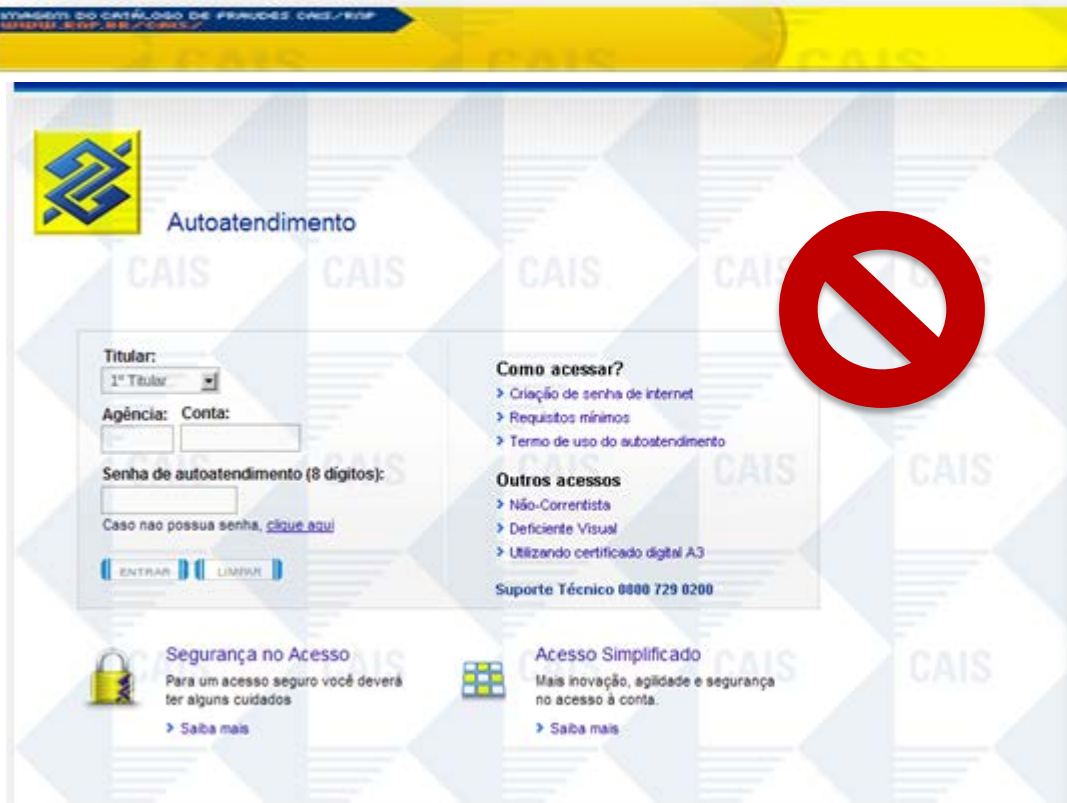


Filename	Content Type	In Cache	Download URL	Browser	Cache Type	Last Accesse...	Last Modified Date	File Size
videoplayback[1...	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v10.lscache6...	Internet Explorer	Web Browser	15/12/2011 16:41:42	18/10/2011 11:56:51	7.122.092
	video/x-flv	Yes	http://www.youtube.com/ptracking?ptk=j...	Chrome	Web Browser	15/12/2011 16:38:04	N/A	0
fla7FDC.tmp		Yes		Chrome	Temporary F...	15/12/2011 16:38:04	15/12/2011 16:38:04	7.122.092
f_000c85	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v10.lscache6...	Chrome	Web Browser	15/12/2011 16:38:04	18/10/2011 11:56:51	7.122.092
	video/x-ms-asf	Yes	http://ad-g.doubleclick.net/adx/com.ytpw...	Chrome	Web Browser	15/12/2011 16:38:04	N/A	466
	video/x-ms-asf	Yes	http://ad-g.doubleclick.net/pfadx/com.ytp...	Chrome	Web Browser	15/12/2011 16:38:03	N/A	6.687
f_000ca3	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v21.lscache5...	Chrome	Web Browser	15/12/2011 16:37:59	28/10/2011 17:39:32	805.908
f_000ca1	video/x-flv	Yes	http://o-o.preferred.tiws-mia1.v12.lscache8...	Chrome	Web Browser	15/12/2011 16:37:32	29/10/2011 16:58:34	838.673
f_000c9f	video/x-flv	Yes	http://v21.nonxt5.c.youtube.com/videopla...	Chrome	Web Browser	15/12/2011 16:37:11	28/10/2011 17:39:32	144.948
fla10E0.tmp		Yes		Chrome	Temporary F...	15/12/2011 16:36:30	15/12/2011 16:36:30	10.905.992



PHISHINGS

Dados – Informação – Conhecimento – Sabedoria




Comunicado falso, em nome do Banco do Brasil, com um link para uma falsa atualização de dados. O link leva ao site falso, destinado a coletar dados da conta bancária da vítima.

Fique atento
ao utilizar o caixa
eletrônico:

- Não aceite ajuda ou atenda pedido de estranhos para voltar ao caixa eletrônico, seu cartão pode ser trocado.
- Ao fim de suas operações, antes de guardá-lo, confira se o nome impresso no cartão é o seu.



PAGAMENTO WEB OU NA BOCA DO CAIXA?

 Bradesco		237-2	Recibo do Sacado		
CEDENTE			CPF/CNPJ	VENCIMENTO	
LD Cedente			20/04/2013	20/04/2013	
NOSSO NÚMERO	NÚMERO DO DOCUMENTO	ESPECIE DOC.	DATA DO DOCUMENTO	AGÊNCIA/COD. CEDENTE	
06/00000000042-8	00042	DM	14/04/2013	0123/0012345-6	
(=) VALOR DOCUMENTO	(-) DEDUÇÕES	(+) ACRÉSCIMOS		VALOR COBRADO	
R\$ 420,00					
SACADO					
LD Teste					
INSTRUÇÃO					
Este é um boleto para demonstração					
			AUTENTICAÇÃO MECÂNICA		


 Corte nesta linha

 Bradesco		237-2	23790.12301 60000.000004 42001.234501 9 56740000042000		
LOCAL DE PAGAMENTO			VENCIMENTO		
Pagável em qualquer agência bancária até a data de vencimento			20/04/2013		
CEDENTE			CPF/CNPJ	AGÊNCIA/COD. CEDENTE	
LD Cedente			20/04/2013	0123/0012345-6	
DATA DOCUMENTO	NÚMERO DO DOCUMENTO	ESPECIE DOC.	ACEITE	DATA PROCESSAMENTO	NOSSO NÚMERO
14/04/2013	00042	DM	N		06/00000000042-8
USO DO BANCO	CARTEIRA	ESP. MOEDA	QUANTIDADE	VALOR MOEDA	(=) VALOR DOCUMENTO
	06	R\$			R\$ 420,00
INSTRUÇÕES					(-) DESCONTOS
Boleto gerado para testes					(-) OUTRAS DEDUÇÕES
Não receber após vencimento					(+) HORA/MULTA
					(+) OUTROS ACRÉSCIMOS
					(=) VALOR COBRADO

SACADO
LD Teste
Rua da Linha, 42
São Paulo - SP - CEP: 99999-999

AUTENTICAÇÃO MECÂNICA/FICHA DE COMPENSAÇÃO



 Corte nesta linha

Boleto verdadeiro ou falso?

Vírus modifica boletos online e faz pagamento cair em outra conta

IGNOW! Da Redação

 Seguir @idgnow

16 de abril de 2013 - 08h00

Ameaça modifica linha digitável dos boletos bancários e inutiliza código de barras. Vírus atinge tanto usuário de internet banking, quanto aqueles que costumam imprimir o boleto

Uma nova ameaça online modifica boletos bancários e faz com que o dinheiro seja creditado em uma conta que não a pretendida pelo usuário. O vírus, identificado pelo site especializado em segurança [Linha Defensiva](#), altera os números da linha digitável e corrompe o código de barras - o que impede o seu uso.


Tanto o valor quanto o vencimento permanecem intáctos, bem como o logotipo do banco - o que impede que a vítima descubra a fraude facilmente. Um dado curioso é que o número do banco é modificado.

Em teste realizado pelo site, o logotipo do boleto pertencia ao Bradesco, mas o número do banco era do Santander - e o mesmo aconteceu com boletos gerados a partir de outros bancos, como Itaú, Caixa Econômica e Banco do Brasil. Mas, segundo o site, "é possível que esse mesmo vírus utilize contas de outros bancos, conforme a necessidade ou interesse dos golpistas", ou seja, mesmo que apenas o número do Santander tenha aparecido nos testes, pode ser que, em outros golpes, o banco de destino seja outro.



POR QUE?



PAGAMENTO WEB OU NA BOCA DO CAIXA?

	Bradesco	033-7	033	Banco Santander (Brazil) SA
CEDENTE		VENCIMENTO		VENCIMENTO
LD Cedente		20/04/2013		20/04/2013
NOSSO NÚMERO	NÚMERO DO DOCUMENTO	ESPECIE DOC.	DATA DO DOCUMENTO	AGÊNCIA/CÓD. CEDENTE
06/00000000042-8	00042	DM	14/04/2013	0123/0012345-6
(=) VALOR DOCUMENTO	(-) DEDUÇÕES	(+) ACRÉSCIMOS		VALOR COBRADO
R\$ 420,00				
SACADO				
LD Teste				
INSTRUÇÃO				
Este é um boleto para demonstração				
AUTENTICAÇÃO MECÂNICA				

Corte nesta linha

	Bradesco	033-7	03399.49380 38000.000000 00423.501014 7 56740000042000		
LOCAL DE PAGAMENTO				VENCIMENTO	
Pagável em qualquer agência bancária até a data de vencimento				20/04/2013	
CEDENTE			CPF/CNPJ		AGÊNCIA/CÓD. CEDENTE
LD Cedente			20/04/2013		0123/0012345-6
DATA DOCUMENTO	NÚMERO DO DOCUMENTO	ESPECIE DOC.	ACEITE	DATA PROCESSAMENTO	NOSSO NÚMERO
14/04/2013	00042	DM	N		06/00000000042-8
USO DO BANCO	CARTEIRA	ESP. MOEDA	QUANTIDADE	VALOR MOEDA	(=) VALOR DOCUMENTO
06	R\$				R\$ 420,00
INSTRUÇÕES					(-) DESCONTOS
Boleto gerado para testes					(-) OUTRAS DEDUÇÕES
Não receber após vencimento					(+) HORA/MULTA
					(+) OUTROS ACRÉSCIMOS
					(=) VALOR COBRADO
SACADO					
LD Teste					
Rua da Linha, 42					
São Paulo - SP - CEP: 11150-120					
AUTENTICAÇÃO MECÂNICA/FICHA DE COMPENSAÇÃO					
					
Corte nesta linha					

<http://www.febraban.org.br/Arquivo/Bancos/sitebancos2-0.asp>

Boleto verdadeiro ou falso?



CAIS - PHISHING

Dados – Informação – Conhecimento – Sabedoria

FRAUDES IDENTIFICADAS

Total de fraudes cadastradas: 4295

1

tipo	FRAUDE - Bradesco	ID: 19511
data	19/02/2013	
assunto	Prezado cliente Bradesco S.A.	
tag	bradesco, bancos, atualizacao	
informações	Imagem 1 - Imagem 2 Texto da mensagem	
arquivo malicioso	Indisponível	
comentário	Phishing: Nessa ocorrencia o fraudador encaminha um email ao usuario informando que sua conta está sendo bloqueada parcialmente e que para desbloquea-la deve acessar o link disponivel no corpo do texto. Desse modo o usuario é encaminhado a uma pagina falsa... (leia mais)	

2

tipo	FRAUDE - Itau	ID: 19496
data	13/02/2013	
assunto	Aviso Final - Sincronizar Dispositivo iToken ,625118	
tag	itau, atualizacao, itoken, bancos	
informações	Imagem 1 - Imagem 2 Texto da mensagem	
arquivo malicioso	Indisponível	
comentário	Phishing: O fraudador encaminha um email ao usuario informando que o dispositivo de segurança do usuario para acesso ao banco está com problemas, mas ao acesar o link disponivel no email é direcionado a uma pagina falsa utilizada na pratica de phishing.	

3

tipo	FRAUDE - Debito	ID: 19501
data	13/02/2013	
assunto	Comunicado Importante - Debito	
tag	debitos, cobranca	
informações	Imagem 1 Texto da mensagem	
arquivo malicioso	2via.exe	
comentário	Malware: Nessa ocorrencia o fraudador encaminha um email ao usuario afirmando que está com debitos pendentes e que para regulariza-lo precisa acessar o link que baixa um software mal intencionado.	

4

tipo	FRAUDE - Banco do Brasil	ID: 19506
data	13/02/2013	
assunto	INFORMATIVO-BB	
tag	bb, bancos, atualizacao, bancodobrasil	
informações	Imagem 1 - Imagem 2 Texto da mensagem	

1

IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/**Bradesco**

Prezado cliente.

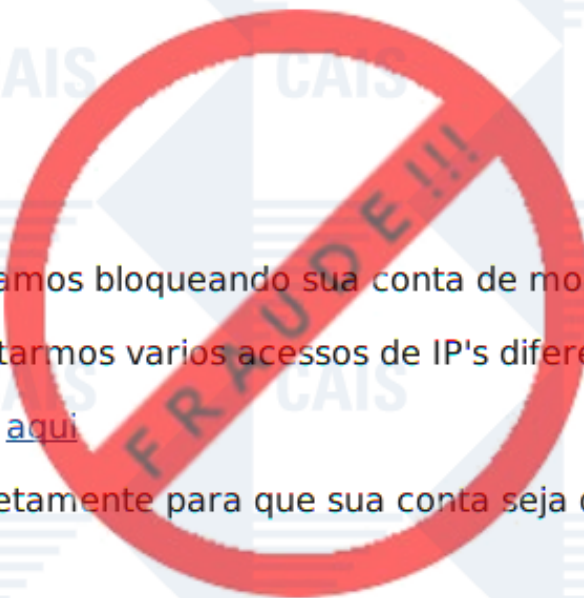
Por motivos de segurança estamos bloqueando sua conta de modo parcial .

Isto acontece devido a constatarmos varios acessos de IP's diferentes em sua conta,

Efetue o desbloqueio clicando [aqui](#)

Lembre-se de preencher corretamente para que sua conta seja desbloqueada corretamente.

Bradesco S.A



2

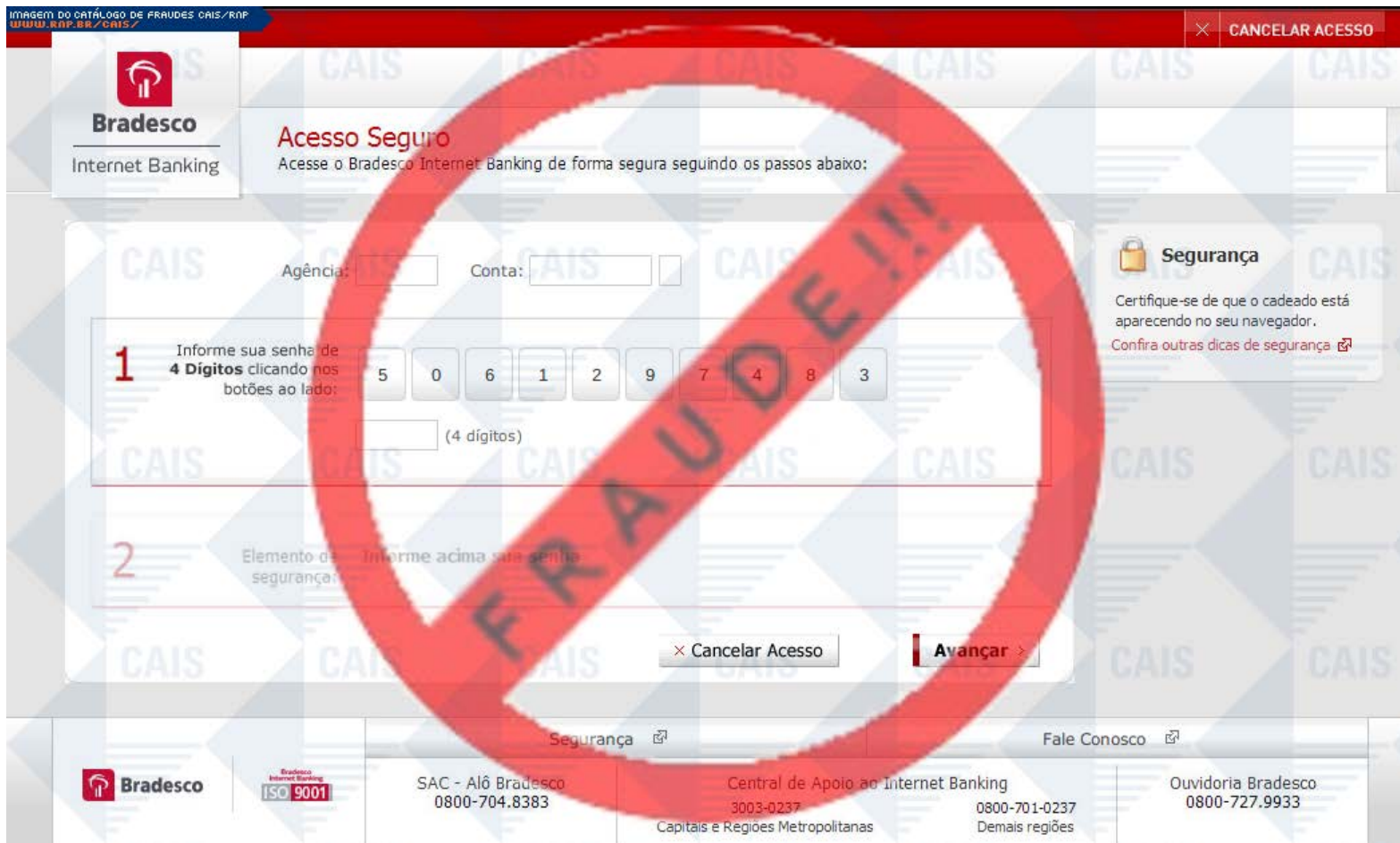


IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
OUVIDORIA RNP BR / CAIS

Cancelar Acesso

Bradesco
Internet Banking

Acesso Seguro
Acesse o Bradesco Internet Banking de forma segura seguindo os passos abaixo:

Agência: Conta:

1 Informe sua senha de **4 Dígitos** clicando nos botões ao lado:

5 0 6 1 2 9 7 4 8 3

(4 dígitos)

2 Elemento de segurança: Informe acima sua senha de segurança:

Segurança
Certifique-se de que o cadeado está aparecendo no seu navegador.
[Confira outras dicas de segurança](#)

Cancelar Acesso **Avançar**

Bradesco **Bradesco Internet Banking ISO 9001**

SAC - Alô Bradesco
0800-704.8383

Central de Apoio ao Internet Banking
3003-0237
Capitais e Regiões Metropolitanas

Fale Conosco

0800-701-0237
Demais regiões

Ouvidoria Bradesco
0800-727.9933

3

IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RAP.BR/CAIS/

Itaú **30** horas Informativo

Queremos lembrar que a conta vinculada ao Contrato de número **09172568362930102-0001** possui um aviso pendente em nosso sistema.

Informamos que seu dispositivo de segurança (**iToken**) encontra-se fora de sincronia.

Para a sua segurança você deve realizar a sincronização de seu aparelho, que tem como finalidade corrigir falhas nos códigos gerados.

* O dispositivo será sincronizado em ambiente seguro através do **Guardião 30 Horas**.

Para iniciar a sincronização clique no botão abaixo:

SINCRONIZAR

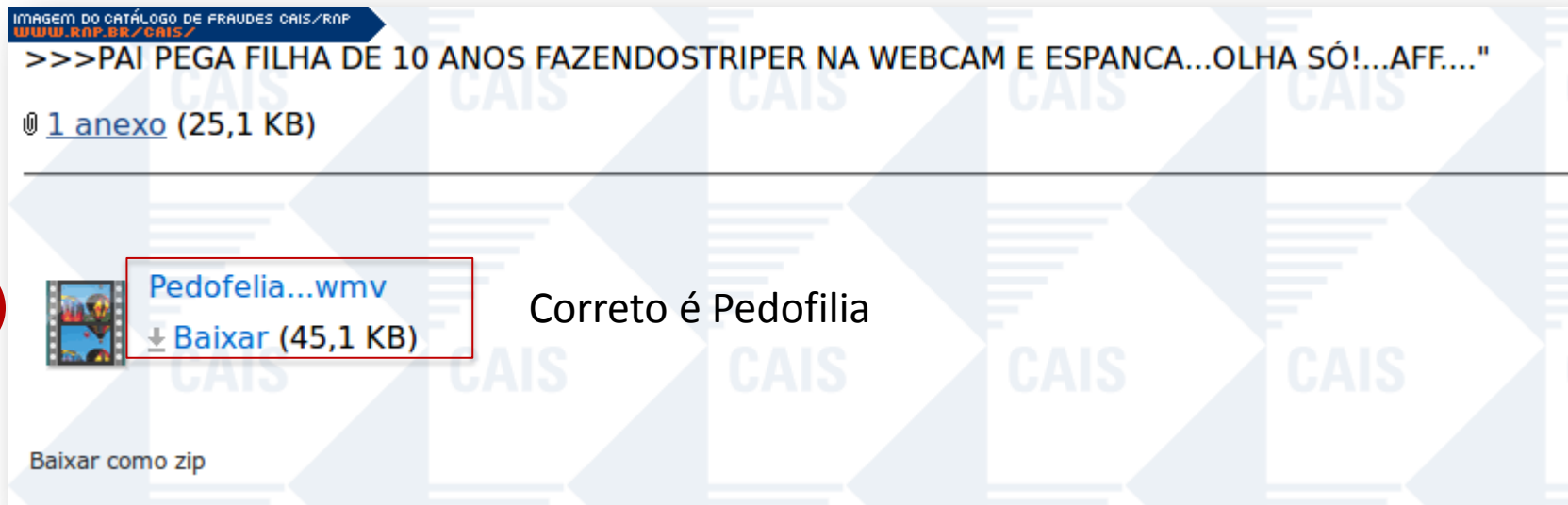
AVISO!

A Atualização do dispositivo é de gênero obrigatória, e deverá ser efetuada até o dia, **14/02/2013**. Caso a sincronização não seja efetuada até a data apresentada, sua conta ficará bloqueada nos canais: Internet, Telefone e Caixas Eletrônicos. O desbloqueio poderá ser feito exclusivamente em sua agência.

  **Itaú**

O Banco Itaú garante o sigilo dos seus dados. Este é um e-mail automático. Não envie resposta. Acesse o site do Banco Itaú e conheça nossa política de privacidade on-line.

Para sugestões e reclamações ligue para o SAC Itaúcard (todos os dias, 24h): 0800 724 4845. Após utilizar esses canais, se desejar a reavaliação da solução apresentada, recorra à Ouvidoria Corporativa Itaú (em dias úteis, das 9 às 18h): 0800 578 0011. Ou seja, ligue para 0800 578 0011.




4

A fraude contém um link para o suposto vídeo com cenas de um pai que espancou a filha após ela ter sido flagrada fazendo striptease na webcam. O link leva ao software malicioso que foi identificado como Gen:Variant.Kazy.54317 (BitDefender).

5

IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/



Seu Cartão Chaves de Segurança Expirou.
O processo de reativação de Chaves de Segurança Bradesco é obrigatório, Para todos os clientes que já utilizam.

Prezado Cliente, [REDACTED]

Informamos que o período de uso das suas chaves de segurança Bradesco expirou. Para continuar utilizando o mesmo Cartão de Chaves e utilizando aos serviços Bradesco como Caixas Eletrônicos, Fone Fácil e Internet Banking, será necessário realizar este procedimento.

Caso a atualização não seja efetuada você precisará comparecer em sua Agência Bradesco e retirar uma nova tabela de senhas. O processo é simples e rápido, basta clicar no endereço abaixo e seguir as instruções.

Para Iniciar o Procedimento, [Clique Aqui](#)

Caso o endereço acima não funcione [clique aqui](#).


Copyright 2012 Bradesco On-line desde 25/05/1995.

Comunicado falso do banco Bradesco informando que o cartão chaves de segurança da vítima expirou. A fraude contém um link que leva a conteúdo malicioso que não estava mais disponível no momento da análise.



PhishTank - PHISHING

Dados – Informação – Conhecimento – Sabedoria



[Sign In](#)

[Register](#) | [Forgot Password](#)

[Home](#) | [Add A Phish](#) | [Verify A Phish](#) | [Phish Search](#) | [Stats](#) | [FAQ](#) | [Developers](#) | [Mailing Lists](#) | [My Account](#)






Join the fight against phishing

Submit suspected phishes. **Track** the status of your submissions.
Verify other users' submissions. **Develop** software with our free API.

Found a phishing site? Get started now – see if it's in the Tank:

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
1745789	http://wrhotels.com/cartao/subscribe.paypal.com-us...	cleanmx 
1745788	http://jxyy.a71.zgsj.net/images/?http://us.battle.n...	cleanmx 
1745787	http://modernfoods.com.cn/js/?dest&	cleanmx 
1745786	http://www.mommytails.com/wp-content/themes/classi...	cleanmx 
1745785	http://creativeoxstudios.com/au/17143f59b6f30db53b...	cleanmx 
1745783	http://creativeoxstudios.com/au/17143f59b6f30db53b...	PhishReporter
1745782	http://codigo1b63f0.com/Visa/index.html	LinhaDefensiva
1745781	http://codigo1b63f0.com/Visa/cadastro.html	LinhaDefensiva
1745779	http://minaseletrica.com.br/css/2/www.hsbc.com.br/...	LinhaDefensiva
1745778	http://minaseletrica.com.br/css/2/www.hsbc.com.br/...	LinhaDefensiva
1745777	http://www.designprint.co.in/form/forms/form1.html	cybercrime

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
[Learn more...](#)

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
[Read the FAQ...](#)

http://service-paypal.confirm.com.websrc/cmdl.login.submit.dispatch.5885d80a.13c0db1f8e263663d3faee8d3.egh50598f678a31312.goldcoastsocialmedia.net/paypal/6b9517c8c4b2c33a3801c3e74



Verificado: É um phish

Conforme verificado por [madsdam cibcrime Metro stuartarant](#)

É um phish 100%
NÃO é um phish 0%

Screenshot do site do local Ver quadro em Ver detalhes técnicos do local Ver em nova janela



The screenshot shows a phishing page designed to look like the PayPal website. At the top, there are navigation links: [Sign Up](#), [Log In](#), [Help](#), and [Security and Protection](#). The main header features the **PayPal** logo and a language selector set to **English**. Below the header is a navigation menu with tabs for **Home**, **Personal**, **Business**, and **Developers**. A secondary menu includes **Get to Know PayPal**, **Pay Online**, **Send Money**, **Get Paid**, and **Products & Services**. On the left side, there is an **Account login** section with input fields for **Email address** and **PayPal password**, a **Go to** dropdown menu set to **My account**, and a **Log In** button. A link for **Problem with login?** is also present. The main content area features a large blue banner with the text **WELCOME TO PayPal** and the tagline **The world's most loved way to pay and get paid. [Learn More](#)**. Below this is a promotional section titled **Get paid anywhere** with the subtext **with your free smartphone card reader**. The image shows a hand holding a card over a blue PayPal card reader.

PhishTank Out of the Net, into the Tank.

[Sign In](#)
[Register](#) | [Forgot Password](#)

[Home](#) | [Add A Phish](#) | [Verify A Phish](#) | [Phish Search](#) | [Stats](#) | [FAQ](#) | [Developers](#) | [Mailing Lists](#) | [My Account](#)

Submission #1745779 is currently ONLINE

Submitted Feb 25th 2013 4:26 AM by [LinhaDefensiva](#) (Current time: Feb 25th 2013 5:39 AM UTC)

<http://minaseletrica.com.br/css/2/www.hsbc.com.br/recadastramento.online/index.php>

Verified: Is a phish

As verified by [buava](#) [fabioassolini](#) [knack](#) [phishphucker](#)

Is a phish **100%**


Is NOT a phish 0%

Screenshot of site

View site in frame

View technical details

View site in new window



The screenshot shows the HSBC website's registration page. At the top, it says "HSBC No Brasil e no mundo, HSBC". Below that is a header "HSBC Recadastramento Online". The main content area is divided into three sections:

- Meu HSBC Internet:** A box asking for the user's CPF to access, with an "Ok" button and a link "Saiba como acessar".
- Connect Bank:** A box with two input fields: "Chave da Empresa:" and "Chave do Operador:", each with an "Ok" button. Below the fields are links "Cadastre-se aqui" and "Saiba mais".
- Segurança para Recadastramento:** A box with a lock icon and text explaining that HSBC asks for total collaboration to ensure security. It includes a link "Saiba mais" and a paragraph about HSBC's commitment to security.

[Friends of PhishTank](#) | [Terms of Use](#) | [Privacy](#) | [Contact](#)

PhishTank is operated by [OpenDNS](#). Learn more about [PhishTank](#) or [OpenDNS](#).

Obrigado!

ERASMO RIBEIRO GUIMARAES JUNIOR -ERGJ

Twitter: @erasmoguilmaras

e-Mail pessoal: eras.com@gmail.com

e-Mail Profissional: guimaraes.junior@menospapel.com.br

Facebook Perfil: ERASMOGUIMARAESJR

Facebook Pagina: Cyber Defesa (Educação, conscientização e prevenção cibernética)

